Vulnerability Identification Errors in Security Risk Assessments

Thesis

Vulnerability Identification Errors in Security Risk Assessments

Stefan Taubenberger BA

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Computer Science

The Open University

Department of Computer Science

Faculty of Mathematics and Computer Science

February 2014

Abstract

At present, companies rely on information technology systems to achieve their business objectives, making them vulnerable to cybersecurity threats. Information security risk assessments help organisations to identify their risks and vulnerabilities. An accurate identification of risks and vulnerabilities is a challenge, because the input data is uncertain. So-called ’vulnerability identification errors‘ can occur if false positive vulnerabilities are identified, or if vulnerabilities remain unidentified (false negatives). ‘Accurate identification’ in this context means that all vulnerabilities identified do indeed pose a risk of a security breach for the organisation. An experiment performed with German IT security professionals in 2011 confirmed that vulnerability identification errors do occur in practice. In particular, false positive vulnerabilities were identified by participants.

In information security (IS) risk assessments, security experts analyze the organisation’s assets in order to identify vulnerabilities. Methods such as brainstorming, checklists, scenario-analysis, impact-analysis, and cause-analysis (ISO, 2009b) are used to identify vulnerabilities. These methods use uncertain input data for vulnerability identification, because the probabilities, effects and losses of vulnerabilities cannot be determined exactly (Fenz and Ekelhart, 2011). Furthermore, business security needs are not considered properly; the security checklists and standards used to identify vulnerabilities do not consider company-specific security requirements (Siponen and Willison, 2009). In addition, the intentional behaviour of an attacker when exploiting vulnerabilities for malicious purposes further increases the uncertainty, because predicting human behaviour is not just about existing vulnerabilities and their consequences (Pieters and Consoli, 2009), rather than preparing for future attacks. As a result, current approaches determine risks and vulnerabilities under a high degree of uncertainty, which can lead to errors.

This thesis proposes an approach to resolve vulnerability identification errors using security requirements and business process models. Security requirements represent the business security needs and determine whether any given

vulnerability is a security risk for the business. Information assets' security requirements are evaluated in the context of the business process model, in order to determine whether security functions are implemented and operating correctly. Systems, personnel and physical parts of business processes, as well as IT processes, are considered in the security requirement evaluation, and this approach is validated in three steps. Firstly, the systematic procedure is compared to two best-practice approaches. Secondly, the risk result accuracy is compared to a best-practice risk-assessment approach, as applied to several real-world examples within an insurance company. Thirdly, the capability to determine risk more accurately by using business processes and security requirements is tested in a quasi-experiment, using security professionals.

This thesis demonstrates that risk assessment methods can benefit from explicit evaluation of security requirements in the business context during risk identification, in order to resolve vulnerability identification errors and to provide a criterion for security.

Author's Declaration

During work on this thesis, several conference and journal papers were published. All of the work presented at conferences, journal papers and in this thesis describes original contributions of the author.

- Taubenberger, Jürjens, Yu, Nuseibeh. "Resolving Vulnerability Identification Errors using Security Requirements on Business Process Models" in *Information Management & Computer Security*, 2013, Volume 21, Issue 3.

  This journal paper contains a condensed view of our literature review (chapter 3) and the concepts of the approach (chapter 4). The approach (chapter 5) as well as its validation (chapter 6) was demonstrated in detail in this paper.

- Taubenberger, Jürjens. "Study on IT risk assessments in practice". *DACH Security conference*, Oldenburg, Germany, September 2011. In proceedings of DACH Security 11, Available at http://www-jj.cs.tu-dortmund.de/jj/publications/papers/dach11-stefan.pdf

  At this security conference, the results of the survey "IT security risk assessments in practice" among German security professionals at a security conference were presented. Some of the survey's results are presented in sections 3.4.2 and 6.5 of this thesis. The complete survey results can be found in the appendix.

- Taubenberger, Jürjens. "Durchführung von IT-Risikobewertungen und die Nutzung von Sicherheitsanforderungen in der Praxis", *Technical report, Fraunhofer Institute for Software and Systems Engineering*, 2011.

In this publication the complete survey „IT security risk assessments in practice" is presented which was conducted among German security professionals. The complete survey results can be found in the appendix.

- Taubenberger, Jürjens, Yu, Nuseibeh. "Problem Analysis of Traditional IT-Security Risk Assessment Methods - An Experience Report from the Insurance and Auditing domain". *Future Challenges in Security and Privacy for Academia and Industry, 26th IFIP TC 11 International Information Security Conference, SEC 2011*, Lucerne, Switzerland, June 2011, Available at http://www.springerlink.com/content/p587547748274275/abstract/

  At his conference, the problems and limitations of information security risk assessment approaches were presented. This publication covers part of the literature review (chapter 3) and the idea of using security requirements for risk assessments (chapter 4).

- Taubenberger, Jürjens. "IT Security Risk Analysis based on Business Process Models enhanced with Security Requirements", *Proceedings of the Workshop on Modelling Security (MODSEC08)* held as part of the 2008 International Conference on Model Driven Engineering Languages and Systems (MODELS). Toulouse, France. 2008. Available at http://ceur-ws.org/Vol-413

  At this conference, an early version of a business process model and security requirements-based assessment approach was presented. This work contains early work of chapters 4 and 5.

Acknowledgements

Special thanks go to my family - to my wife Katrin for supporting me all the time, and my daughters Stefanie and Magdalena. I hope you will excuse me for the time I was not available for you, especially in the first years of your life, because of working on the PhD.

I wish to thank my supervisors Jan Jürjens, Yijun Yu and Bashar Nuseibeh for their invaluable guidance, reviews, and encouragement to finish this thesis. Especially, I like to thank Jan Jürjens, because without him, the PhD would not have been possible. He supported and encouraged me during the whole project, from the end of 2006. His availability and his kindness were prominent and a great source of motivation. I thank him for all his trust and support. Furthermore, I would like to thank warmly my second supervisor Bashar Nuseibeh. He has always supported my PhD; his open-mindedness and his warmth were always a great help to me. In addition, I wish to thank Yijun Yu for his excellent ideas and discussions we had, specifically on the subject of combining risk management with software engineering. His comments were always a great source of inspiration to my work. Moreover, I would like to thank Marian Petre for her valuable reviews and comments on this thesis.

Finally, I must acknowledge the support of the Computing Department of The Open University and the Technical University of Dortmund. Without the universities' departments - as well as other PhD students of both universities giving me time, support and encouragement - this thesis would not have been

completed. Finally, I must thank my employer, especially the Audit and Integrated Risk Management department, for supporting my PhD throughout the period of time, as well as for being a source for gathering practical experiences and data.

Table of Contents

Figures and Tables

Acronyms

ALE - Annual loss expectancy

APRA - Australian Prudential Regulation Authority

AS/NZ - Australia/ New Zealand Standards

BAFIN - Bundesanstalt fuer Finanzdienstleistungsaufsicht

BPM - Business Process Model

BPMN - Business Process Modeling Notation

BS - British Standard

BSI - Bundesamt für Sicherheit in der Informationstechnik

CAPEC - Common Attack Pattern Enumeration and Classification

CC - Common Criteria

CC - Communication Channel

CCE - Common Configuration Enumeration

CCTA - Central Computer and Telecommunications Agency

CERT - Computer Emergency Response Team

CMM - Capability Maturity Model

COBIT - Control Objectives for Information and Related Technology

CORAS - Risk Assessment of Security Critical Systems

COSO - Committee of Sponsoring Organisations of the Treadway Commission

CPQRA - Chemical Process Quantitative Risk Assessment

CRAMM - CCTA Risk Analysis and Management Method

CRM - Customer Relationship Management

CVE - Common Vulnerabilities and Exposures

CVSS - Common Vulnerability Scoring System

DFD - Data Flow Diagrams

EBIOS - Expression of Needs and Identification of Security Objectives

ENISA - European Network and Information Security Agency

EP - Entry Point

EPC - Event-driven Process Chain

EVT - Extreme Value Theory

FMECA - Failure Mode and Effects Analysis

FSA - Financial Service Authority

FTA - Fault Tree Analysis

GAISP - Generally Accepted Information Security Principles

HAZOPS - Hazard and Operability Study

HIPAA - Health Insurance Portability and Accountability Act

IDEF - Integration Definition

IEC - International Electrotechnical Commission

IS - Information Security

ISF - Information Security Forum

ISMS - Information Security Management System

ISO - International Organisation for Standardization

IT - Information Technology

ITIL - IT Infrastructure Library

ITSEC - Information Technology Security Evaluation Criteria

KAOS - Knowledge Acquisition in Automated Specification

MARION - Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux

MEHARI - Methode Harmonisée d'Analyse du Risque Informatique

MTD - Maximum Tolerable Downtime

NIST - National Institute of Standards and Technology

OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation

OGC - Office of Government Commerce

PCAOB - Public Company Accounting Oversight Board

PHA - Preliminary Risk Analysis

PP - Process Point

PRA - Probabilistic Risk Assessment

PROLOG - A logic programming language

RE - Requirements Engineering

RM - Risk Management

SE - Software Engineering

SEC - Securities and Exchange Commission

SEI - Software Engineering Institute

SO - Security Objective

SOX - Sarbanes-Oxley Act

SP - Special Publication

SPICE - Software Process Improvement and Capability Determination framework

SQL - Structured Query Language

SQUARE - Security Quality Requirements Engineering

SR - Security Requirement

SSE CMM - Systems Security Engineering Capability Maturity Model

TCSEC - Trusted Computer System Evaluation Criteria

TR - Technical Report

UML - Unified Modelling Language

UMLsec - An extension to the Unified Modelling Language

VAR - Value-at-risk

Chapter 1 - Introduction

In this chapter, the motivation for the research and the problem statement are presented, and the research objective is discussed with the aid of information security models developed by other researchers.

1.1. Motivation

In 2007, two data discs containing 25 million child benefit records were lost in the United Kingdom (Hartnett, 2007), and 45.7 million credit card numbers were stolen by hackers at TJX, a retailer located in Massachusetts, USA (Brodkin, 2007). Information security risk assessments are performed to identify such risks caused by vulnerabilities before they occur, and to propose security functions. A risk is defined as “the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation” (ISO, 2004b, p. 7), and a vulnerability can be defined as “a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy” (Stoneburner et al., 2002b, p. 15). However, both the identification of information security risks and the proposing of mitigating security functions are dependent on the accurate identification of vulnerabilities. Accurate identification in these contexts means that those identified vulnerabilities can indeed result in a security breach and are a security risk for the organisation. Vulnerability identification errors do occur when a vulnerability is either wrongly identified (false positive) or unidentified (false negative).

As a first step in any information security risk assessment, assets, threats and vulnerabilities are identified according to standards from the Standards Australia/Standards New Zealand Committee (AS/NZS), the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC), for example: AS/NZS ISO 31000 (ASNZ, 2009) (formerly AS/NZS 4360 (ASNZ, 1999) and including ISO/IEC 31000 (ISO, 2009a)); ISO/IEC 27001 (ISO, 2005d) and ISO/IEC 27005 (ISO, 2011c). The ISO/IEC 13335-1 (ISO, 2004b) defining basic security concepts was replaced by ISO/IEC 2700x series.

In these standards, procedures and techniques such as brainstorming, checklists, scenario-, impact-, and cause-analysis are proposed to identify threats and vulnerabilities. Furthermore, the determination of critical business processes (Khanmohammadi and Houmb, 2010) and information assets (Stevens, 2005) was proposed, in order to establish an asset and its value for an organisation (Stevens, 2005). Security requirements (Gerber and von Solms, 2001) have also been introduced, describing the level of security needed, and identifying the most suitable security functions, the criticality and impact of the risks and vulnerabilities. However, the knowledge used by security experts at these assessments, such as checklists or security-related best practices, is uncertain; often, statistical data for threats, occurrence or impact are not available, incomplete or possibly wrong (Fenz and Ekelhart, 2011). In addition, vulnerabilities documented in knowledge bases are not specific to the company’s activities and security needs (Siponen and Willison, 2009), which can lead to ignorance of the vulnerabilities or, in some cases, determining too many. Although security requirements help to judge any vulnerability from a business perspective, they are not explicitly evaluated for discovering and resolving vulnerabilities.

Vulnerability identification errors can lead to unwanted losses, or can cause a company to invest in security functions that are not required. However, the successful and accurate identification of vulnerabilities can make the company more cost-efficient with regard to spending on security. It can prevent image and/or financial loss (Carg et al., 2003), and can help to demonstrate adherence to business security needs as well as any governmental regulations (Luthy and Forcht, 2006) and privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA) (HIPAA, 1996).

In this thesis, a new method is proposed that applies existing concepts, such as information assets and security requirements, to business process models (BPMs). Business process models describe the activities of a process in an organisation to achieve an objective. From the BPMs, one can first identify information assets, actors and systems for a risk assessment. For each information asset, the criticality in the form of security objectives can be determined by business process objectives. Thereafter, security requirements refining the security objectives can be elicited and used to argue for the correct identification of vulnerabilities. The security functions relating to business process activities, where the information asset is processed, are compared against the security requirements, so as to identify vulnerabilities. The novelty is the explicit evaluation of security requirements as against security functions within business process models for vulnerability identification, in order to resolve identification errors (false positives, false negatives and true positives). However not all vulnerability identification errors might be eliminated by applying the approach.

1.2. Problem statement

The protection of information, and identifying risks to information needs adequate processes in place. Information security risk assessment encompasses the activities used to identify and evaluate risks to information. In information security risk assessments, threats and vulnerabilities (representing a risk) are identified by security experts using information gathering techniques such as questionnaires, checklists, interviews, document reviews, scenario-, impact- and effect-analysis, brainstorming, etc. (ISO, 2009b). In addition, they employ scanning tools to identify threats and vulnerabilities. These techniques use security and vulnerability knowledge bases, where the knowledge base can be the security expert itself, or any available best security practices, security advisories or vulnerability lists issued by public or private organisations and companies. But these security knowledge bases are generic in scope, and are not tailored to the security needs of a particular organisation (Siponen and Willison, 2009). Vulnerabilities are identified by comparing the content in knowledge bases, or the possible scenario/threat as against the actual implementation of security functions. Companies' security processes, systems or security functions are checked as to whether the vulnerability exists, and as to whether security functions, described in security knowledge bases, are being implemented. The vulnerability identification procedure performed is based on the principle "you know one if you see one", which implies an implicit matching process.

Conversely, the accurate identification of vulnerabilities with this procedure is a challenge, as it is virtually impossible to verify whether all vulnerabilities have been identified correctly in a given environment. This is because the knowledge used by

security experts is uncertain and unspecific with regard to the company's security needs; moreover, implicit information is used and can hardly be reproduced. However, the required security described by security requirements could be used for a more accurate identification of vulnerabilities. Because security requirements specify what should be achieved and indicate necessary security functions, they can be the baseline for any judgment on a security issue for the organisation. Figure 1-1 below illustrates the problem of identifying vulnerabilities accurately (i.e. the security needs of an organisation).

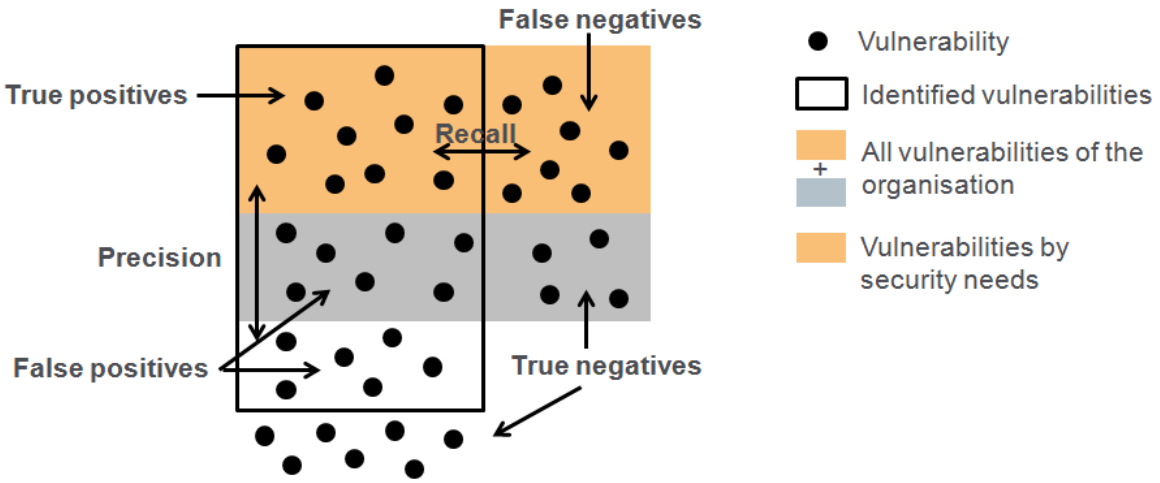


Figure 1-1 Vulnerability identification errors

In an information security risk assessment a number of vulnerabilities are identified – they are represented by black dots within the black rectangle in Figure 1-1. There are some which are not identified at all (outside the rectangle), some to which the organisation is not vulnerable (blank area in and outside the rectangle) and some to which the organisation is vulnerable (orange and dark grey area) but which do not represent a vulnerability (dark grey area). Vulnerabilities within the dark grey area or the blank area of the rectangle are false positives. False positives are vulnerabilities identified which do not represent an actual vulnerability for the organisation (blank area of the rectangle), but where the organisation might be vulnerable (dark grey area of the rectangle). Those in the dark grey or blank

area outside the rectangle are true negatives not identified as vulnerabilities. The vulnerabilities within the orange area of the rectangle represent true positives. True positives are correctly identified vulnerabilities (as defined by security needs). Vulnerabilities outside the rectangle and within the orange area are false negatives. False negatives are not identified but are actual vulnerabilities to which the organisation is vulnerable. Recall is the ratio of accurately (defined by security needs) identified vulnerabilities and unidentified vulnerabilities out of all the accurate vulnerabilities (orange area) of an organisation. Precision is the ratio between true positives and false positives - the ratio of accurate identified vulnerabilities. As we elaborate in the literature review (chapter 3), in current procedures, asset-specific security requirements are not evaluated against security functions to identify (positive) vulnerabilities.

1.3. Research objectives

The objective of this research is to consider the required security - business security needs - in vulnerability identification, in order to enable security experts to identify (positive) vulnerabilities accurately, and to validate the method developed in this research. Accurate, in this context, means the identification of flaws or weaknesses that can result in a security breach or a violation of a security policy and which are thus a security risk for the organisation. The difference between the proposed method and existing approaches, which already use security requirements, is the explicit evaluation of security requirements within the business context - at business process models - to identify vulnerabilities accurately. Security requirements are used as the foundation for identifying vulnerabilities defining the required security (similar to security best practices), for comparing the security function implementation and identifying vulnerabilities. The

advantage of this proposal is that the security requirement specification defines the security of the organisation and and can be used as an overall measurement value for security; to identify true positives and help to resolve false positives and false negatives.

The foundation of this research is information security models which describe the concepts used (e.g. assets, vulnerabilities, and security requirements) in information security risk management and assessment. Researchers that have defined an information security risk model, like Innerhofer–Oberperfler and Breu (2006), use the model to present the basic concepts of information security and how they use them in their enterprise architecture risk assessment approach. Stølen et al. (2002) use a model to represent the relationships between the risk assessment terminologies used in CORAS. Matulevicius et al. (2008) provide a reference model defining the concepts of information security risk management, which was consolidated from existing security standards and used to improve Secure TROPOS. According to their research, risk-related concepts describe how risk is defined by concepts such as threats, vulnerabilities and impact. Asset-related concepts describe important assets and their security, whereas risk treatment-related concepts describe the decisions, requirements and security functions used to mitigate risks. Hereafter, these models are presented to show the relations between concepts such as vulnerabilities, risk and security requirements, in order to finally define our research objective. A relationship in these models connects elements used in the model and describes their nature to others. Text annotations and arrows or associations are used to represent these relationships. An element represents a concept (e.g. risk) or part of the concept

(e.g. vulnerabilities, threats and events). Mostly, elements are represented as text boxes or by modelling notations such as the unified modelling language (UML).

The security concept meta-model of Innerhofer–Oberperfler and Breu (2006) in Figure 1-2 shows that a security requirement is derived from a business security objective and attached to a model element that is basically an asset. A threat violates the security requirements and targets an asset. Security controls treat threats.

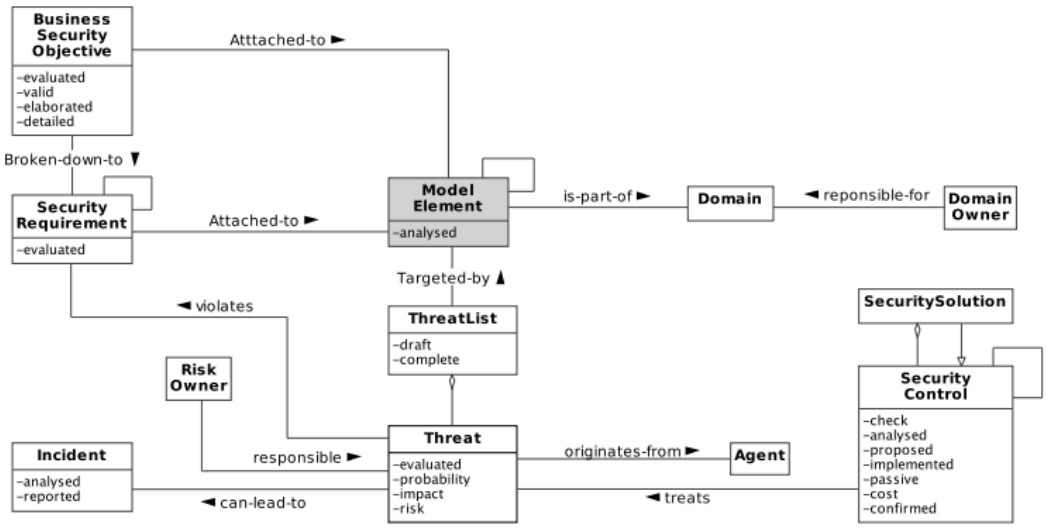


Figure 1-2 Extended Security Concept Meta-Model from Innerhofer–Oberperfler and Breu (2006)

The terminology model of Stølen et al. (2002) in Figure 1-2 shows that a threat may exploit a vulnerability of an asset, thereby causing a risk. Security requirements are formulated in the security policies that protect an asset and reduce vulnerabilities. The target of evaluation that contains assets should satisfy security requirements.

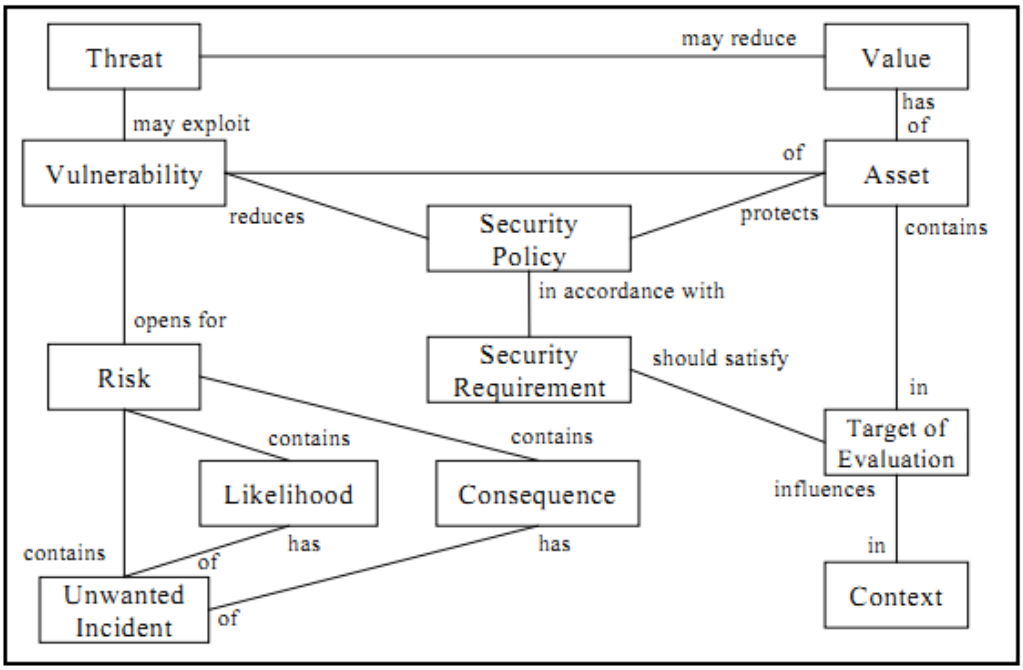


Figure 1-3 Terminology model from Stølen et al. (2002)

In the information system security risk management (ISSRM) reference model of Matulevicius et al. (2008) in Figure 1-3, a control implements a security requirement that thus mitigates a risk (defined as a threat that exploits a vulnerability that in turn leads to an impact). The impact of a threat harms an asset. The different colours of model elements in the model show the content of asset-related concepts (cyan), risk-related concepts (orange) and risk treatment-related concepts (green).

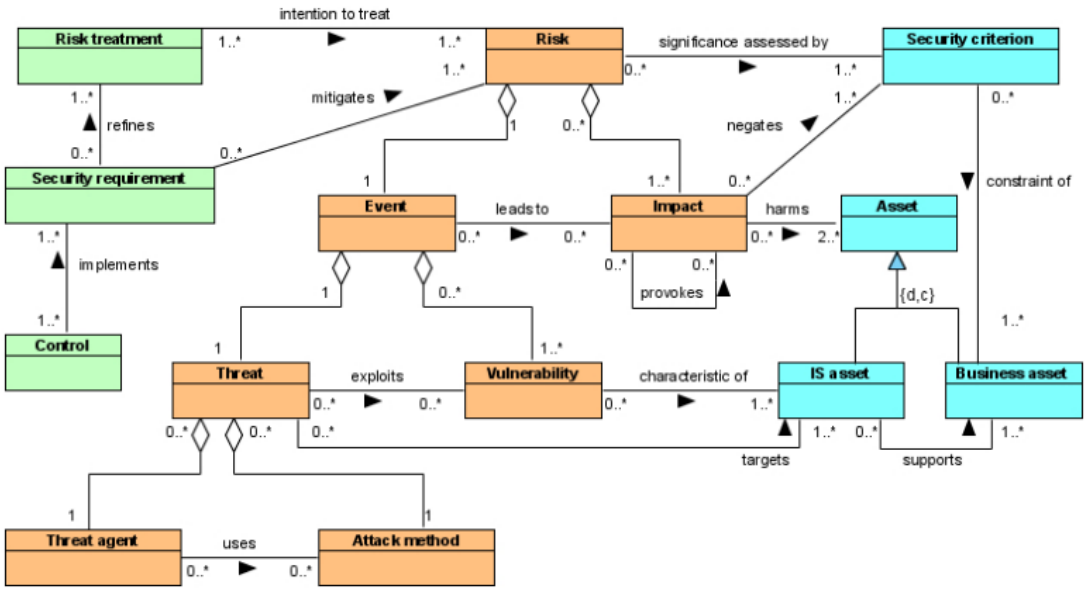


Figure 1-4 The ISSRM reference model from Matulevicius et al. (2008)

The objective of this research is to consider the security required in vulnerability identification, and therefore the focus is on the relationship between security requirements, assets, vulnerabilities and risks. All the above models show that security requirements are attached to assets, and mitigate or reduce a risk in respect of vulnerabilities. A risk or vulnerability is mitigated by a corresponding security function - e.g. administrative, physical, and technical controls - that implements the security requirement. If a security function is not implemented fully or correctly, the risk or vulnerability is not mitigated - the asset is at risk - and the security requirements are not adhered to. Thus, non-adherence to security requirements would indicate a vulnerability, and it is therefore hypothesised that the explicit evaluation of security requirements can be used for the resolution of vulnerability identification errors (false positives and false negatives), as only vulnerabilities with regard to business security needs would be identified. Resolving vulnerability identification errors would help to reduce security costs spent on inefficient security measures, as well as to demonstrate that business

security needs are adhered to (in other words, that the company is secure and compliant).

1.4. Structure of this thesis

This thesis is organised into various chapters; Figure 1-5 provides an overview.

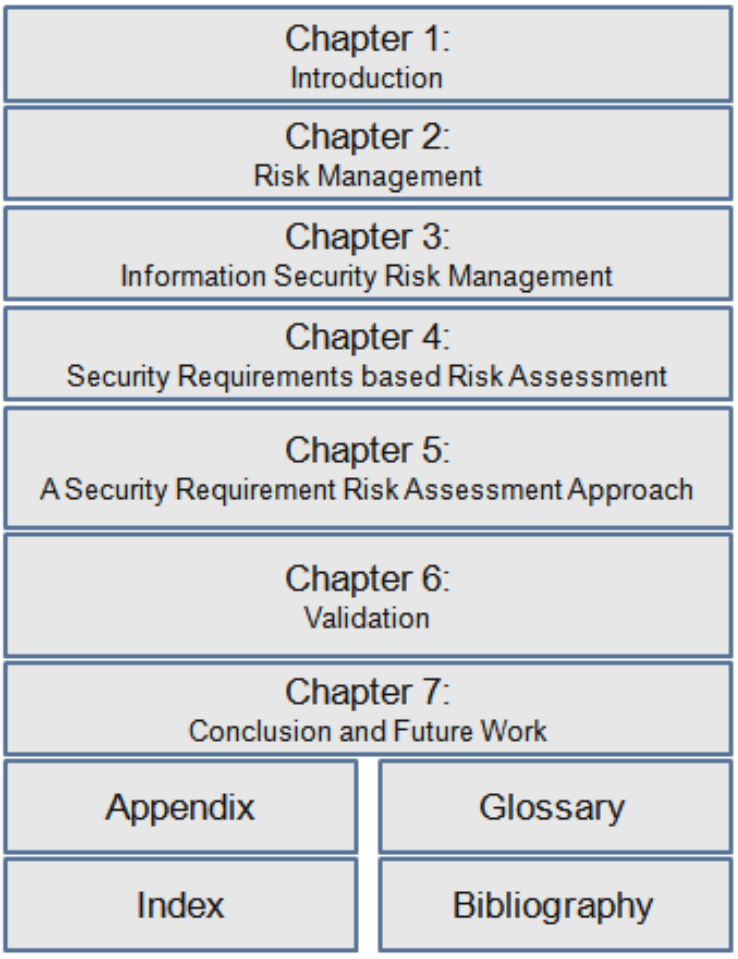


Figure 1-5 Structure of the thesis

In chapter one, an introduction to the problem is given and the research objective outlined.

In chapter two, background information is provided about risk management. The main standards for (information security) risk management are presented.

Furthermore, the terminology and main activities of information security risk assessments are explained.

Chapter three contains the literature review. An overview of information security risk assessment standards and methods is provided. The literature is evaluated, to demonstrate how security requirements and business process models are utilised in current approaches to determine information security risks in the information security, security requirements engineering and business process model domains. The focus of the literature review is on whether security requirements are utilised, and if so, how they are used to determine vulnerabilities in information security risk assessments. In addition, a survey was performed of German security professionals at a security conference, to identify the limitations of current security risk assessments in practice. Finally, based on the literature review, the research questions were developed.

Chapter four is about concepts in information security risk assessment and management. An extended information security model was compiled from the existing models presented in the introductory chapter; it shows how concepts in security risk assessments and risk management are related. In addition, a definition of risk based on security requirements is provided and how security requirements, business process models and information assets can be used for resolving vulnerability identification errors is also explained. Furthermore, the elicitation of security requirements is discussed and a structure for security requirements' characterisation presented based on business process model information supporting the assessment process.

In chapter five, the proposed security requirements risk assessment approach called ‘SRA’ using security requirements and business process models for vulnerability identification is described in detail. By employing an example, each step of the proposed approach is explained.

Chapter six is about the validation work. The SRA was validated by method comparison, testing and a quasi-experiment. Three validation criteria were defined for the validation of the approach, namely method procedure (how systematic security requirements are currently evaluated in assessments); result accuracy (how accurate the risk results of our proposed approach are); and method capability (whether security requirement and business process model information can decrease vulnerability identification errors).

Chapter seven concludes with an overview of the research contribution, potential areas for future work, and concluding remarks about the research presented in this thesis.

Chapter 2 - Risk Management

This chapter presents background information about (information security) risk management and the risk assessment process as well as defines terminology. A definition of terms used in this thesis can be found in the glossary.

2.1. Areas of risk management

Risks - the possibility of adverse or unwelcome circumstances - are and have always been a part of our daily life. Therefore, risk analysis and risk assessment is not a new area of research and has a long tradition. The origin of risk management - to identify, analyse, evaluate and treat risk - in the early modern and industrial age goes back to the 16th century. The formation of the first fire insurance business after the Great Fire of London in 1666 and the foundation of marine insurance by Edward Lloyd (today Lloyds of London) in the 1680s formed the origin of insurance business. These initial insurance policies covered fire risks and transportation risks. Other forms of insurance, like the first social and health insurance, were founded in the mid-17th century, only covering disability and distressed widows. The main commonalities of insurance policies are that they cover risks in class of homogeneous exposure units and concentrate on the occurrence of an event causing a measureable financial loss. The price for the insurance cover is based on statistical data, market price, or gut feeling if no data is available. The insurance business has survived over centuries and nowadays a huge range of insurance policies are offered. An important point to note is that insurance companies always evaluate for a special portfolio of risks - stated in the insurance policy - where they have enough statistical data; they exclude certain

risks or events where they do not have enough statistical data or have suffered outstanding losses, e.g. for terrorism. This enables them to provide an insurance policy and to determine a suitable price for the insurance cover.

In the engineering field, risk analysis methods like the failure mode and effects analysis (FMEA/FMECA) (NASA, 1966) were developed by the US Military in the 1950s to classify failures that could affect the success of mission, personnel or the equipment. Also, fault tree analysis (FTA) (Ericson, 1999) was an outcome of a military project for a missile launch control system to evaluate the safety of the system. FTA is a logical diagram of system failures and their impact on the components of the system. The probabilistic risk assessment (PRA) (Stamatelatos, 2000) was developed by the nuclear industry in the 1960s to determine risks of complex engineered entities, especially to assess for reactor safety. In the 1970s, the PRA was then adopted by the chemical industry to determine chemical process incidents; it was named as the chemical process quantitative risk assessment (CPQRA) (Arendt, 1990). In the engineering field, the term safety is used to mean the protection against hazards. Hazards are risks or events that threaten human lives, the environment, production or materials. Most commonly, safety is related to risks that affect human life or environmental health (Lautieri et al., 2005). Risk is defined by the severity of adverse events and the probability of the occurrence of each event.

In the financial sector, there are two main streams for risk management: firstly, to limit losses of financial institutions, and secondly to protect stakeholders from material misstatements in financial reports. Methods like Value-at-risk (VAR) (Jorion, 2006) or extreme value theory (EVT) (Diebold et al., 1998) have been

applied to financial portfolios to limit losses of financial investments; these all use statistical theories and data to determine their maximum loss in the case of an event. Over the last two decades, risk management standards and regulations have been published for stakeholder protection as a result of bankruptcy or of fraud in business companies. Standards, such as the Committee of Sponsoring Organisations of the Treadway Commission (COSO, 1994) I and COSO II (COSO, 2004) defining enterprise risk management activities; the Australian/New Zealand Risk Management Standard 4360 (ASNZ, 1999) about risk management, and laws like Sarbanes-Oxley (Sarbanes-Oxley Act, 2002) for controls in financial reporting, Basel II (Basel Committee on Banking Supervision, 2004) for capital requirements for banks or Solvency II (European Commission, 2007) for capital requirements for insurance companies were all published. The aim of these regulations and standards is to oblige companies to identify, to manage and to inform about risks. Nowadays, regulations like Basel II, Solvency II or the Sarbanes-Oxley act are the main drivers for companies to determine and manage risks categorised as market, reputation, strategic or operational risks within these regulations.

In the computing domain, the first security standards were developed in the 1980s to protect information and data. The first of its kind was the Trusted Computer System Evaluation Criteria (TCSEC) (US DoD, 1988) for the evaluation of the effectiveness of computer security controls - referred to as Orange Book. It was developed for the US Department of Defense (DoD) in 1983. Further standards on computer security followed at the beginning of the 1990s. For example, the German security criteria (ITS) - now the baseline protection manual (BSI, 2008) - for evaluation and certifying computers and software in 1989, or the European Information Technology Security Evaluation Criteria (ITSEC) (European

Communities, 1991) for certifying the functionality and confidentiality of software and computer systems regarding data- and system-security in 1991. The British Standard 7799 (UK DTI, 1995) was the origin of current information security standards, published in 1995, and evolved from the BS 7799 to ISO 17799 (ISO, 2005b), to ISO 27001 (ISO, 2005d) and then to ISO 27002 (ISO, 2005e) in more recent times. In computing, the focus of risks is on security, i.e., threats and the protection of information. A threat can be unintended, or deliberate - i.e., someone has an intention to get some benefit out of the action (Albrechtsen, 2003). These actions are often planned and conducted by malicious users. Therefore, security is related to the protection of information against these threats, where information may be changed, accessed without authorisation, destroyed, made unavailable or disclosed. The protection of information concerns the confidentiality, integrity and availability of information and identification of threats and vulnerabilities compromising these security objectives. Security investments are closely related to the protection of information, but are not the focus of this thesis. Security investments - applying cost-effective security functions - should reduce the risks threatening assets balanced by costs for security and incidents (ENISA, 2012). Return on Security Risk Investment and Annual Loss Exposure (Sonnenreich et al., 2006), decision support models (Beresnevichiene et al., 2010) and trade-off analysis (Loannidis et al., 2012) were also suggested to determine the ‘optimal’ amount of investments in security.

To conclude, the analysis and assessment of risks is conducted in various areas and focuses on different aspects within these fields. The common baseline of risk management approaches is the objective to determine risks and to mitigate them to an acceptable level for the organisation. This thesis concentrates on risk

assessments in the computing area, determining information security risks for businesses.

2.2. Standards

In risk management, the first published and acknowledged standard is the AS/NZS 4360 (ASNZ, 2004) which provides the input in terms of concepts or terminology for any other standards. AS/NZS 4360 is a risk management standard published by the Standards Australia/Standards New Zealand Committee (AS/NZS). It was first published in 1999 and was revised in 2004. In 2009 the AS/NZS 4360 was superseded by the AS/NZS ISO 31000 (ASNZ, 2009). The AS/NZS risk management standard provides a generic framework for managing risk, as well as definitions of terms. Within the standard, risk management activities are described that can be applied generally, to any organisation or domain. The objective of the standard is to identify opportunities and risks, to provide a basis for decision-making, to support pro-active management, and to improve compliance and corporate governance. The main elements of the risk management process are shown in Figure 2-1 and involve establishing the context, identifying risks, analysing and treating risk, monitoring and reviewing, as well as communicating and consulting. These process activities have not changed from AS/NZS 4360 to AS/NZS ISO 31000; therefore, in the following reference is made solely to AS/NZS 4360.

(a) Establish the context: “Establish the external, internal and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis defined.” (ASNZ, 2004, p. 7).

(b) Identify risks: “Identify where, when, why and how events could prevent, degrade, delay or enhance the achievement of the objectives.“ (ASNZ, 2004, p. 7).

(c) Analyse risks: “Identify and evaluate existing controls. Determine consequences and likelihood and hence the level of risk. This analysis should consider the range of potential consequences and how these could occur.” (ASNZ, 2004, p. 7).

(d) Evaluate risks: “Compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities.” (ASNZ, 2004, p. 8).

(e) Treat risks: “Develop and implement specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs.” (ASNZ, 2004, p. 8).

(f) Monitor and review: “It is necessary to monitor the effectiveness of all steps of the risk management process. This is important for continuous improvement. Risks and the effectiveness of treatment measures need to be monitored to ensure changing circumstances do not alter priorities.” (ASNZ, 2004, p. 8).

(g) Communicate and consult: “Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.” (ASNZ, 2004, p. 7).

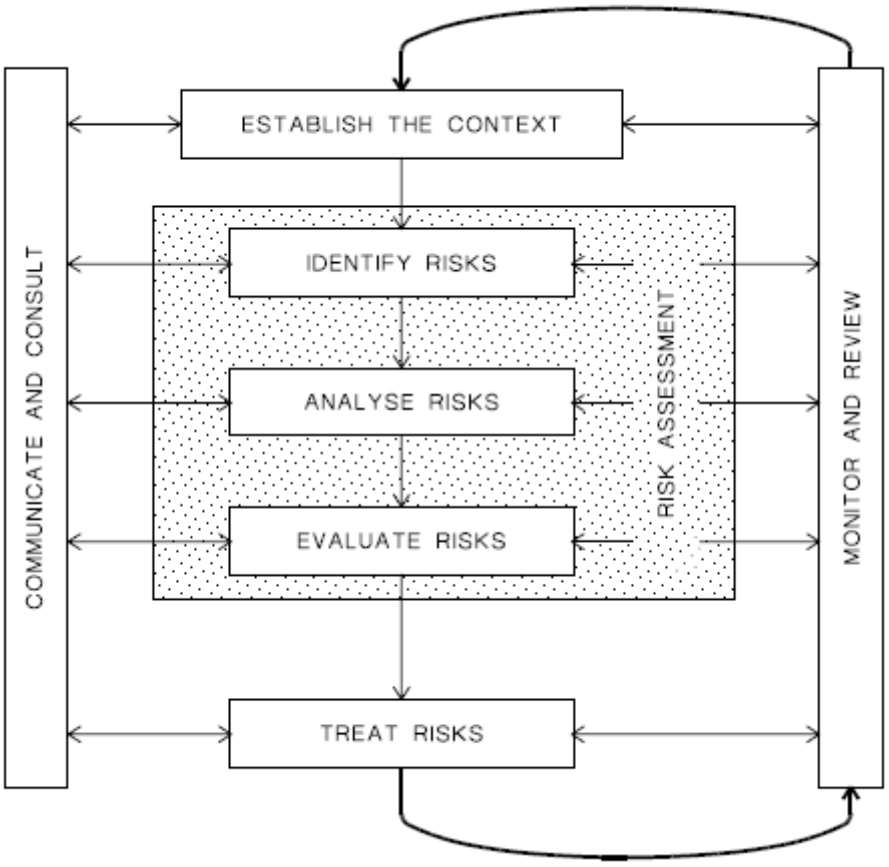


Figure 2-1 Risk management process from ASNZ (2004)

ISO/IEC 31000:2009 and ISO/IEC 31010:2009

The ISO/IEC 31000:2009 - Risk management - (ISO, 2009a) issued by the International Organisation of Standardisation (ISO) in 2009 provides principles and generic guidelines for risk management. The main difference to AS/NZS 4360 is that the risk management process is further extended by a risk management framework and risk management principles (see Figure 2-2). Furthermore, risk was re-defined as “the effect of uncertainty on objectives” (ISO, 2009a, p. V). The standard describes the principles for managing risks, and provides a management framework for risk as well as the risk management process. It claims to be usable by public, private or community enterprises, associations, groups or individuals for their risk management activities. The relationship between the principles for

managing risk, the framework in which it occurs and the risk management process as indicated in ISO/IEC 31000:2009 is shown in Figure 2-2. The principles, shown on the left of the Figure, describe high-level principles that should be adhered to by all functions in an organisation achieving effective risk management. The framework (in the middle of the figure) defines process steps assisting in managing risks effectively; these should be integrated in the overall management system. At the framework, recurring process activities are defined for identifying and reporting risks, as well as the decision-making process on risks. The risk management process (to the right of the figure) defines the activities for identifying, analysing and reporting of risks. The risk management process is similar to that defined in AS/NZS 4360. The ISO/IEC 31000 was adopted by the Standards Australia/Standards New Zealand Committee and published as AS/NZS ISO 31000.

The ISO/IEC 31010:2009 - Risk assessment techniques - (ISO, 2009b) provides guidance on the selection and application of systematic techniques for risk assessment. This standard provides no specific criteria for risk identification but describes activities for identifying risks along the risk management process defined in ISO/IEC 31000. It also provides a comparison of risk assessment techniques and their strengths/limitations. The standard contains a list of methods, a description of the method and indicates the area of applicability. Both standards, the ISO/IEC 31000 and 31010, provide the foundation of principles and techniques for risk management and assessment.

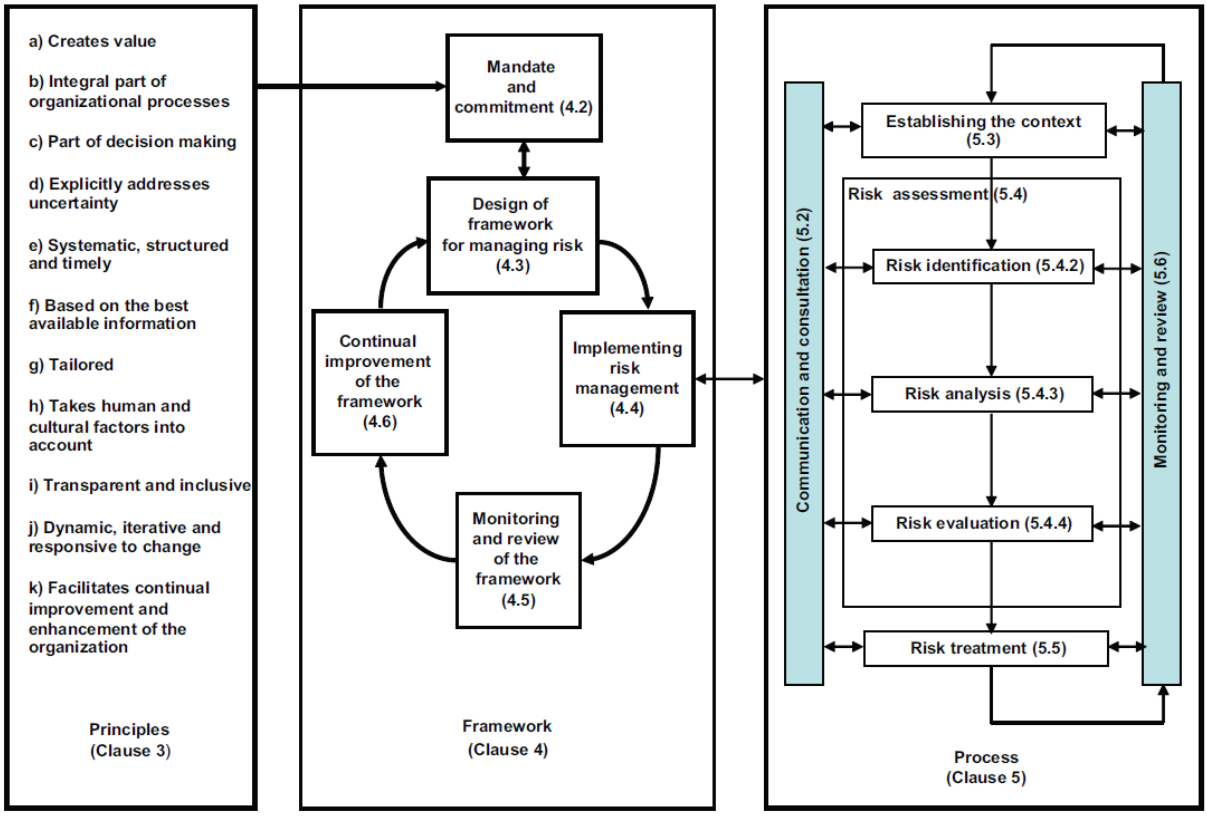


Figure 2-2 Risk management framework, principles and process from ISO/IEC 31000 (ISO, 2009a)

ISO Guide 73:2002

The ISO Guide 73:2002 (ISO, 2002) issued by the International Organisation of Standardisation (ISO) provides basic and generic definitions of terms associated with risk management. The aim of this guide is to promote a coherent approach to the description of risk management activities and the use of risk management terminology. It primarily assists in the communication process, in that it defines a basic terminology for risk management. Although the ISO Guide 73 is about risk management, it is frequently referenced to in information security literature. The ISO Guide 73:2002 is superseded by the ISO/IEC 27000:2009 (ISO, 2012).

2.3. Information security

Organisations use information that is created and processed by persons and systems in processes in order to achieve their business objectives. For an organisation, it is critical to protect and to secure this information, which presents a value. In the past, security was mainly associated with data and systems and not with information. However, the understanding of security changed from a systems view to an information view in computer science, over time.

> *"Data security became computer security, and computer security became IT security and IT security became information security because of the better understanding of the business impact and associated risk of not properly protecting a company's electronic resources"* (von Solms and von Solms, 2005, p. 272).

The expression 'data security' evolved over time to 'information security' because of the closer alignment of computer systems with business operations and financial accounting processes requiring the protection of business information. In the ISO 17799:2005 (ISO, 2005c), information security is defined as the "preservation of confidentiality, integrity and availability of information … other properties such as authenticity, accountability, non-repudiation, and reliability can be involved" (ISO, 2005c, p. 1). Because of the closer alignment of business processes and computer systems, any loss of confidentiality, integrity and availability of information can now cause more severe adverse effects to an organisation and their business objectives. Therefore, information has to always be adequately protected. The protection of information, identifying security needs as well as risks to information, needs adequate processes in place. Information security risk management is about the processes taken to identify, evaluate and

mitigate risks, with the objective to protect and to manage the security of information within the organisation. The different process activities in information risk management are: establish the context, risk assessment, risk treatment, risk communication and risk monitoring (ISO, 2011c). In this thesis, the focus is on risk assessment - identifying and evaluating risks with regard to the specific information of an organisation. Before the risk assessment process activities for information security are explained, definitions for confidentiality, integrity, availability and risk are provided.

Confidentiality

Confidentiality ensures that information is not made available to unauthorised entities (ISO, 2005c) and is concealed (Bishop, 2002). It is the prevention of unauthorised disclosure (European Communities, 1991).

> *"Confidentiality ensures that computer related assets are accessed only by authorised parties. That is, only those who should have access to something will actually get that access. By 'access', it is meant not only reading but also viewing, printing, or simply knowing that a particular asset exists. Confidentiality is sometimes called secrecy or privacy"* (Pfleeger and Pfleeger, 2002, p. 10).

Availability

Availability ensures that resources are accessible and usable on demand by authorised entities (ISO, 2004b).

> *"Availability means that assets are accessible to authorised parties at appropriate time. In other word, if some person or system has legitimate access to a particular set of objectives, that access should not be prevented.*

> *For his reason, availability is sometimes known by its opposite, denial of service"* (Pfleeger and Pfleeger, 2002, p. 10).

It is the safeguarding that information or resources are not obtained by unauthorised entities (European Communities, 1991).

Integrity

Integrity is the protection of the accuracy and completeness of assets (ISO, 2004b).

> *"Integrity means that assets can be modified only by authorised parties or only in authorised ways. In this context, modification includes writing, changing, changing status, deleting and creating"* (Pfleeger and Pfleeger, 2002, p. 10).

It is about protecting information of unauthorised or improper modifications (European Communities, 1991; Bishop, 2002).

Risk definition

Any threats that affect the confidentiality, integrity and availability of information are a risk for an organisation. Generally in risk management, risk is defined as "the chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood" (ASNZ, 1999, p. 3). This definition has changed, in AS/NZS ISO 31000, to "the effect of uncertainty on objectives" (ASNZ, 2009, p. 1). In information security, risk is defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the asset (i.e. an impact)" (Ciechanowicz, 1997, p. 225).

This definition has changed a little in relation to assets. In the National Institute of Standards and Technology's (NIST) special publication (SP) about risk management, risk is defined as "a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organisation" (Stoneburner et al., 2002b, p. 8). In ISO 27000 (ISO, 2012, p. 4) information security risk is defined as the "combination of the probability of an event and its consequence". Information security risks are defined by threats, vulnerabilities and their impact to an asset. A risk is therefore characterised by a threat that uses a vulnerability of an asset which has an impact to the organisation. The severity of a risk is dependent on the impact. In this thesis, the term risk is understood as defined in ISO 31000: "the effect of uncertainty on objectives" (ISO, 2009a, p. 1).

Risk assessement process activities

The risk assessment process activities as defined in standards like AS/NZ 4360 (ASNZ, 2004) or ISO 31000 (ISO, 2009a) are also applicable for information security, as the objective is to identify and assess risks. The single activities in a risk assessment are risk identification, risk analysis and risk evaluation (ISO, 2004b) analogous to the risk management processes of AS/NZS 4360. In the following, these activities are described with specific regard to information security.

Establish the context

Establish the context is a prepatory step for a risk assessment. Assets such as physical assets (hardware), software, data, people and intangibles (e.g. goodwill) are the basis of every risk assessment. An asset can comprise of anything that has value to an organisation (ISO, 2004b). In information security, assets can be

hardware, software and information to be protected against threats. These assets have to be identified in the ‘establish the context’ phase of a risk assessment, as do their value and their sensitivity for the organisation. Therefore, the business objective - the organisation’s mission - has to be considered to value assets and to evaluate risks. Some approaches have introduced security requirements and/or risk measurement criteria that are identified in the ‘establish the context’ phase, and then used in later phases of the risk assessment. These security requirements and/or risk measurement criteria can be seen as constraints affecting the organisation and determining its information security orientation. They can also be used as criteria for determining the impact of vulnerabilities or risks.

Risk identification

In the risk identification phase, risks are identified by questions like “what can happen?”, “what could go wrong?” or “how it can happen?”. Therefore, events, threats and vulnerabilities that can have a negative impact or lead to security breaches are identified for an asset. A threat can be defined as “a potential cause of an incident that may result in harm to a system or organisation” (ISO, 2004b, p. 3). In other ISO standards, a threat is described as either “of natural or human origin, … accidental or deliberate.” It “may arise from within or the outside of the organisation” (ISO, 2011c, p. 14). Breu and Innerhofer-Oberperfler (2005, p. 4) define a threat as “any event that can result in the violation of a security requirement.” A vulnerability can be defined as “a flaw or a weakness that can be exercised and results in a security breach” (Stoneburner et al., 2002b, p. 15), or as “a weakness of an asset or group of assets that can be exploited by one or more threats” (ISO, 2004b, p. 3). In this thesis a threat is defined as defined in ISO

(2012) as a potential cause of an unwanted incident (exercising a vulnerability), which may result in harm to a system or organization.

The identification of threats and vulnerabilities is conducted by the security expert using information gathering techniques, for example, questionnaires, on-site interviews, document reviews, scenario analysis or scanning tools. The identification of vulnerabilities is based on the matching of knowledge bases to the security control implementation. These knowledge bases are the security expert, security best practices or vulnerability lists. Such lists include vulnerability databases like CVE (known vulnerabilities of systems), scoring systems like CVSS (rating an identified vulnerability), attack patterns like CAPEC (descriptions of common methods for exploiting software) and secure system configuration lists like CCE (unique identifiers to security-related system configuration issues).

Risk analysis

After vulnerabilities have been identified, the impact and probability of being utilised by a threat for each is estimated. Vulnerabilities which are classified as low may be removed from this analysis. To determine the impact as well as the probability of being utilised by a threat not an easy task. Possible sources of information for estimates can be publications, internal data, market investigations and expert estimations. Qualitative and quantitative methods can be used to evaluate impact and probabilities of vulnerabilities and threats.

Risk evaluation

The estimated level of risk for threats and vulnerabilities that was determined in the process activity before, should now be compared against measurement criteria. The output of this process activity is the risks that should be reduced and treated.

In the main, qualitative measurement criteria such as high, middle and low are employed, which were already used in the risk analysis. After all risks have been evaluated, decisions have to be made as to which risks are treated by developing security functions or risk mitigation strategies. A security function is a countermeasure or a control that avoids, reduces, transfers or retains risks to a defined level. Countermeasures or controls can be selected from available information security standards or can be designed to meet specific requirements. A countermeasure or control can be a policy, a procedure, a guideline, practices or organisational structures; it can be of administrative, technical or legislative nature (ISO, 2005c). A security policy is a description, or a set of policies, that defines how organisations' assets are protected with regard to information security. Security policies are further refined by security procedures, guidelines or practices.

2.3.1. Risk assessment

The academic community, as well as businesses and governmental organisations, have developed numerous approaches for information security (IS) risk assessment. Existing IS risk assessment approaches were developed in general and for specific domains. That is to say, there are approaches for special domains or single aspects like project management (Luqi and Nogueira, 2000), operation systems/networks (Manadhata and Wing, 2005), health-care (Warren, 2001), e-commerce, business process reengineering (Herrmann and Herrmann, 2006), different phases of the risk management process (Bandyopadhyay et al., 1999), lifecycles (Bernard, 2007), considering specifics of the domain or a specific problem. But business and governmental organisations have also developed a broad range of IS security risk assessment approaches. These approaches differ in the abstraction level and in the proposal of security functions. Some of these

approaches formulate high-level security policies or general security requirements, whereas others specify detailed technical solutions or parameters for IT systems. In these approaches, a catalogue of basic protection measures (BSI, 2008) is provided, or best practices for security control objectives and processes (ISSA, 2004); the information security risk management process (ISO, 2011c) is explained, or guidance on risk management activities for IT systems (Stoneburner et al., 2002b) provided. Sometimes, even the settings for IT infrastructure components are stipulated (Stoneburner et al., 2002a). A discussion and review on these approaches can be found in Ralston et al. (2006) who reviews approaches for critical infrastructure systems, Mayer (2009) who reviews information security risk management standards and methods, and Hogganvik (2009) on security risk analysis methods and techniques. A comprehensive list of public available risk assessment methods can be found in the publication of the ENISA ad-hoc working group on risk management and assessment (ENISA, 2006), at ENISA's website (ENISA, 2013) and that of the Information Security Working Group of the US House of Representatives (Putnam et al., 2004).

However, this diversity of the developed approaches causes the problem of how to classify these approaches according to both their extent, as well as their objectives. This classification problem is discussed and clarified in section 2.3.3. 'Risk assessment method classification'. A commonality of all approaches in the academic, business and governmental field is that they rely on quantitative or qualitative methods, or on both (Rainer et al., 1991). In the following, the key advantages and disadvantages of quantitative and qualitative methods are illustrated.

Quantitative risk assessment methods use numeric probability, where the probability expresses the knowledge that the event occurs. With quantitative approaches, risk is determined by the probability of an event and the likelihood of a loss. Examples of the use of quantitative methods are: normal probability, Bayesian probability, fuzzy theories and Dempster Shafer theory, Monte Carlo simulation, annual loss expectancy (ALE), and stochastic dominance. The advantages of such methods are that assets are identified most likely for damages (Rainer et al., 1991), measures can be used for the impact magnitude and they can thus be directly compared (Feather and Cornford, 2006). The disadvantages are that there are no exact probability values of loss at the time when they are estimated, and half of the estimates are statistically either too high or too low (Rainer et al., 1991). Furthermore, the probability function that usually follows a normal distribution may be deformed, because values recorded may represent the average of a few extremes and many low values (Rainer et al., 1991). Additionally, a scale has to be provided for what the value of “x” percent means (Stoneburner et al., 2002b) and these values have to be given a literal meaning.

Qualitative risk assessment methods use non-numeric values or number ranges to express risk as a descriptive value (Rainer et al., 1991). Examples for qualitative methods are: scenario analysis, fuzzy metrics, questionnaires, preliminary risk analysis (PHA), hazard and operability study (HAZOPS), and failure mode and effects analysis (FMEA/FMECA) (see Rausand, 2004). The advantages of qualitative methods are that they are time- and cost-efficient, because no exact value has to be determined and they are valuable in estimating risk approximately (Rainer et al., 1991); areas of improvement can also be easily identified (Stoneburner et al., 2002b). However, their key disadvantage is that they

are not precise - the value is expressed within a spectrum that has to be understood by all involved parties (Rainer et al., 1991). Additionally, methods provide no measurement for the impact and therefore, it is difficult to conduct a cost-benefit analysis (Stoneburner et al., 2002b). Although quantitative and qualitative methods can be combined and used in conjunction (Zhang et al., 2010), the combination of results and their interpretation become more difficult because of different rating scales, underlying assessment principles, or the variances in risk weighting.

2.3.2. Risk assessment vs. analysis

In many publications regarding IT security risk assessment, the terms risk analysis and risk assessment are often used simultaneously, to express the identification of events and the evaluation of impact and probability. For example, Aagedal et al. (2002) refer to risk assessment as “incorporating risk analysis and risk management, i.e., it combines systematic processes for risk identification and determination of their consequences, and how to deal with these risks”. In the paper of the ENISA ad-hoc working group on risk management and assessment (ENISA, 2006), the authors distinguish only between risk assessment and risk management methods. For example, the CCTA Risk Analysis and Management Method (CRAMM) (CCTA, 1987) was classified as a risk assessment method whereas Warren (2001) refers to it as a risk analysis method. According to Gerber and von Solms (2001), the main objective of risk analysis is “to identify and assess all risks and then to suggest a set of controls that will reduce these risks to an acceptable level”. Stelzer (2002) defines risk analysis as the identification and evaluation of endangering events, as well as their causes and consequences. Rainer et al. (1991) refer to risk analysis as “the process managers use to

examine the threats facing their IT assets and the vulnerabilities of those assets to the risks". Risk analysis, meanwhile, "consists of identifying IT assets, identifying threats to those assets, and determining the vulnerability of asset(s) to threat(s)" (Rainer et al., 1991, p. 133).

In all the papers of the paragraph above, the authors do not distinguish between risk analysis and risk assessment. They either use risk analysis or risk assessment for identification and evaluation of threats and impacts. Sometimes they include activities of risk management - e.g. the mitigation and control of risk - in their definitions. However, there are differences in the activities associated with the terms risk analysis, risk assessment and risk management. In 1987, Guarro had already distinguished between risk assessment and risk analysis; he defined them as follows:

> *"This term [risk assessment] is today mostly used to indicate the analytical activities by which the nature of the threats potentially affecting a system, and the severity of the consequences that may result from them, are investigated and evaluated. The closely related term risk analysis is employed in a more technical context, usually to indicate the more detailed procedures employed by specialists to dissect risk into its more specific constituents, e.g. the relations among threats, assets, damage or loss consequences and countermeasures."* (Guarro, 1987, p. 494).

Rausand (2004) distinguishes between risk analysis, risks assessment and risk management in the following way. Risk analysis includes scope definition, hazard identification and risk estimation; on the other hand, risk assessment incorporates risk tolerability decisions and analysis of options. Risk management is about risk reduction/control and involves decision-making, implementation and monitoring.

In the ISO/IEC Guide 73:2002 (ISO, 2002), they distinguish between risk analysis, risk assessment and risk management. Risk analysis is defined as the systematic use of information to identify sources and to estimate the risk; risk assessment as overall process of risk analysis and risk evaluation; and risk management as coordinated activities to direct and control an organisation with regard to risk. In the ISO 31000 (ISO, 2009a), risk assessment is the overall process of risk identification, risk analysis and risk evaluation. Risk analysis is the process to comprehend the nature and level of risk.

In this thesis, the term risk assessment is used as defind in the ISO 31000 (ISO, 2009a), to identify, analyse and evaluate risks.

2.3.3. Risk assessment method classification

In general “published work related to risk assessment is very difficult to categorise” (Ralston et al., 2006, p.6), and “there are more than 200 risk management methods making it a challenge to select the most adequate one” (Matulevicius et al., 2008, p.1). These difficulties to categorise and select an appropriate risk assessment approach arise because the risk management process consists of different activities: risk identification, risk analysis, risk assessment (evaluation and ranking) and risk management (treatment and mitigation) and approaches cover different activities. Furthermore, they concentrate on different aspects, problems or business areas - for example, one issue in classifying approaches is to determine how much of the risk assessment activity is covered by the developed approaches. Another is the great variety and profundity of the approaches. Campbell and Stamp (2004) developed a classification scheme - a matrix - for risk assessment methods, which revolves around their complexity and usability. The matrix consists

of two dimensions (level and approach) divided further into subcategories. With their matrix, the scope (abstract, mid-level, concrete) and the approach (comparative (e.g. best practice), functional (e.g. assistant) and temporal (e.g. exercise)) can be assessed, but it lacks a classification regarding the elements of the risk assessment approach. Siponen (2005) analysed the current IS security approaches and research regarding underlying assumptions and features of IS methods; previously, Dhillon and Backhouse had done the same (1996) in regard to key characteristics of research efforts in information systems security. Siponen (2005) classified the approaches in checklists, standards, maturity criteria, risk management and formal methods. These five basic classes miss out on any further distinguishing characteristics and are therefore not expedient for a classification. Dhillon and Backhouse used the categories: checklists, risk analysis and evaluation. Even if their aim was to promote research in the security domain for interpretive and empirical studies, a clear distinction between the approaches (apart from a basic categorisation into checklists and approaches) is not provided by either. Sunyaev et al. (2009) also provides a classification scheme with five categories: checklists, assessment approaches, risk analysis approaches, IT security management approaches, and legislation accommodations. This method provides distinguishing attributes for the classification of approaches in one of these categories, but the subcategories used are not further annotated. Furthermore, there are overlaps between the categories (like assessment and risk analysis approaches) in their description, which are unexplained. These overlaps make it difficult to classify an approach according to the given, basic classification. In a paper of the ENISA ad hoc working group on risk assessment/risk management (ENISA, 2008) as well as in Pöttinger (2009), risk exposure, risk impact and impact segment are used to determine the most appropriate risk

assessment methodology. Spider diagrams are used to compare the methods with organisational requirements.

To summarise, currently there is no general accepted and proven classification scheme for existing risk assessment approaches. Further, developed or criticised approaches are typically not classified or categorised, which makes it hard for researchers to apply the approach in the correct setting or to select the most appropriate one. For the literature review in this thesis, information security risk assessment standards and security risk assessment methods are the only distinguishing factors made - as by other researchers (Mayer, 2009). Standards represent high level references for risk management and assessment, and describe the risk management process from a procedural perspective. These standards contain the definitions for risk assessment and are the basis for any developed methods by researchers or organisations. Security risk assessment methods define and describe risk assessment activities in detail, how to assess risks in a particular area or situation by proposing a procedure of activities to be performed. Only these two categories are used in the literature review in chapter 3 to distinguish between the approaches found in the literature.

2.3.4. Security requirements at risk assessments

The assessment and protection of information of an organisation is not only about considering concerns of confidentiality, integrity and availability by identifying threats and vulnerabilities. It is also about the security required - business security needs - to address these concerns (Gerber et al., 2001). The required amount of security can be defined by security requirements. However, to use security requirements for risk assessments (especially for identifying vulnerabilities and

risks based on the required security), a definition is needed of security requirements.

In information security risk assessments, security requirements are defined as the level of protection needed in regard to the security concerns of confidentiality, integrity, availability, auditability and authenticity (Bishop, 2003), or types and levels of protection to meet the security policy (Brinkley and Schell, 1995). The security requirements definition of Gerber and von Solms (2001) - to consider also the required security from a business perspective, regulatory or statutory requirements and applicable laws as well as risk to infrastructure - was not adopted in other security definitions. In another paper of Gerber et al. (2001), a security requirement is defined as the combination of security concerns (confidentiality, availability, integrity, accountability and authentication) and intensity level.

Innerhofer-Oberperfler and Breu (2005) define a security requirement as “a detailed description of security properties of a specific model element. Depending on the model element type, it can be a detailed technical specification of a high level description of security properties at the business level. A Security Requirement must be derived from a Security Objective.” A security objective is defined as “a high level, abstract definition of the goal of security management” (Breu and Innerhofer-Oberperfler, 2005, p. 4). In another paper of Breu et al. (2008), regarding risk analysis of health care networks, they redefine the definitions of security objective and security requirements. “A Security Objective describes the overall security goals of the system, in particular, general legal requirements, specific availability and integrity requirements of various institutions and privacy requirements of patients” and “a Security Requirement is a detailed

context-dependent explication of a Security Objective. It breaks a Security Objective down into several more detailed descriptions. The context of a Security Requirement is derived from the model element for which it is defined. Security Requirements are linked to Security Objectives to depict paths of inheritance. Security requirements may be described informally by text…" (Breu et al., 2008, p. 4).

Herrmann and Herrmann (2006) also distinguish between security objectives and security requirements but in their work, security objects are security requirements concerning the element of a business process. They use a predefined list of security requirements, such as confidentiality, integrity, availability, anonymity, pseudonymity, privacy and authenticity, that are assigned to business process elements.

Siponen and Oinas-Kukkonen (2007) defines four security requirements - namely, integrity, confidentiality, availability and non-repudiation - that are relevant for information security.

The ISO 17799 (ISO, 2005c) states that the sources relating to the determination of security requirements for assessing risks are business objectives, legal and regulatory requirements, and principles and objectives of an organisation to support operations. However, an exact definition of security requirements is not given. In another paper of Gerber and von Solms (2008), where they examine the legal sources to derive security requirements, they refer to the security requirements definition of ISO 17799.

In the software engineering field, security requirements describe the necessary security for systems to protect against threats. Firesmith defines a security requirement as "typically a detailed requirement that implements an overridden

security policy” (Firesmith, 2003, p. 54). Moffett et al. (2004) define security requirements as “constraints on functional requirements that are needed to achieve security goals”. In contrast, Matulevicius et al. (2008) define it as “the refinement of a treatment decision to mitigate the risk”. In a publication of Haley et al. (2008), security requirements are also defined as a function of constraints. Based on a survey of different security requirements definitions in the software engineering domain, Tondel et al. (2008) argue that there is no current agreement on what a security requirement is, as well as whether security measures should describe a security requirement. But, they recommend the description of requirements in respect of what should be achieved - not how it should be done.

This (as well as the survey of Tondel et al. (2008)) shows that a generally accepted definition of security requirements is not available. The differences in the definitions of security requirements derive from the main focus of both domains. Software engineering is concerned with the development of systems based on requirements, whereas information security risk assessment is concerned more with the identification and mitigation of risks of an organisation. As there is no generally accepted definition in the literature, the perspective of the software engineering domain is followed. In this thesis a security requirement represents constraints on the functions of the system, where these constraints operationalize one or more security objectives (Haley et al., 2008). The definition, elicitation and characterisation of security requirements for information security risk assessment with business processes are described in section 4.5.

Chapter 3 - Information Security Risk Management

The literature review focuses on journal articles, conference proceedings, specific books, theses and technical reports in the computing area with regard to information security (IS) risk assessments for an organisation. IS risk assessment standards and methods are presented, as developed by organisations and researchers. Those methods are discussed which use security requirements and business process models in the information security, security requirements engineering and business process model fields, and how the security requirements are used there. Furthermore, limitations of security risk assessments are discussed with an example, as well as with the results of a survey performed among security professionals. This chapter concludes with the research questions to be answered and the validation methods used.

3.1. State of practice

In the following information security risk management standards are distinguished from information security risk assessment methods. Besides risk management standards, like AS/NZ 4360 (ASNZ, 2004) and ISO 31000 (ISO, 2009a) described in section 2.2, these standards describe the concepts of information security risk management, define risk terminology, and form the basis of any developed methods. Methods describe activities to be performed and techniques used for the risk assessment activities defined in the standards.

3.1.1.Risk management standards

Information security standards act as the reference point and foundation for any developed methods, as well as providing the basis for the terminology and concepts used therein. The standards were mainly developed or supported by public or governmental organisations and finally resulted in an ISO/IEC standard, as described below.

ISO/IEC 13335-1:2004

The ISO/IEC 13335-1:2004 (ISO, 2004b) standard, issued by the International Organisation of Standardisation (ISO), “deals with the management aspects of planning, implementation and operations, including maintenance, of information and communications technology (ICT) security” (ISO, 2004b, p. 5). The standard explains risk concepts and provides advice on organisational aspects of information security management. The ISO/IEC TR 13335 part 1 (of 1996) and part 2 (of 1997) were combined into the revised ISO/IEC 13335-1:2004. The parts ISO/IEC TR 13335-3:1998 and the ISO/IEC TR 13335-4:2000 were superseded by the ISO/IEC 27005:2008 (ISO, 2011b), revised in 2011, which is specifically about information security risk management. ISO/IEC 13335-1:2004 was withdrawn in 2010 with the release of the ISO/IEC 2700x series, which is about information security.

The ISO/IEC 2700x series

The ISO/IEC 2700x series issued by the International Organisation of Standardisation (ISO) consists of a number of standards to do with information security management. “An information security management system (ISMS)

provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets. [The aim of this is] to achieve business objectives based upon a risk assessment and the organisation's risk acceptance levels, designed to effectively treat and manage risks" (ISO, 2012, p. 7). These standards cover information security management broadly, starting with basic vocabulary, and continue to define specific guidelines and processes for implementing and monitoring security concepts. The following standards were published:

- ISO/IEC 27000:2012 — Information security management systems — Overview and vocabulary (ISO, 2012). This standard describes the overview and the vocabulary of information security management systems and defines related terms.
- ISO/IEC 27001:2005 — Information security management systems — Requirements (ISO, 2005d). This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System. The standard specifies requirements for the implementation of security controls customised to the needs of the organisation and designed to ensure the selection of adequate and proportionate security controls that protect information assets.
- ISO/IEC 27002:2005 — Code of practice for information security management (ISO, 2005e). This standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organisation. The standard contains best practices of control objectives and controls for information security management.

- ISO/IEC 27003:2010 — Information security management system implementation guidance (ISO, 2010). This standard focuses on the critical aspects needed for successful design and implementation of an information security management system (ISMS). It also describes the processes of specification, design and implementation of an ISMS.
- ISO/IEC 27004:2009 — Information security management — Measurement (ISO, 2011a). This standard provides guidance on the development and use of measures and measurement to assess the effectiveness of an implemented information security management system (ISMS) and controls, or groups of controls.
- ISO/IEC 27005:2011 — Information security risk management (ISO, 2011c). This standard provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk-management approach.
- ISO/IEC 27006:2011 — Requirements for bodies providing audit and certification of information security management systems (ISO, 2011d). This standard specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS). It is primarily intended to support the accreditation of certification bodies providing ISMS certification.
- ISO/IEC 27011:2008 — Information security management guidelines for telecommunications organisations based on ISO/IEC 27002 (ISO, 2011e). This standard is about guidelines supporting the implementation of information security management in telecommunications organisations.

- ISO/IEC 27031:2011 — Guidelines for information and communications technology readiness for business continuity (ISO, 2011f). This standard describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify aspects (such as performance, design and implementation) for improving an organisation's ICT readiness.
- ISO/IEC 27033 — Network security (ISO, 2011g). The first part of this standard provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security. The second part gives guidelines for organisations to plan, design, implement and document network security. The third part describes the threats, design techniques and control issues associated with reference network scenarios.
- ISO/IEC 27035:2011 — Security incident management (ISO, 2011h). This standard provides an approach to detect, assess, report, respond to and manage information security incidents. Moreover, it provides guidance to detect, to assess and to manage information security vulnerabilities; it helps to continuously improve information security and incident management.
- ISO 27799 — Information security management in health using ISO/IEC 27002 (ISO, 2011i). This standard provides guidelines for specifying a set of detailed controls for managing health information security and security best practice guidelines with regard to health information.

ISO/IEC 15408:2009

The ISO/IEC 15408:2009 “Information technology -- Security techniques -- Evaluation criteria for IT security” is a revision of ISO/IEC 15408:2005, also known as Common Criteria (CC) (CC, 2006). The common criteria consist of: ISO/IEC 15408-1:2009 (Part 1 - Introduction and general model), ISO/IEC 15408-2:2008 (Part 2 - Security functional components) and ISO/IEC 15408-3:2008 (Part 3 - Security assurance components). The ISO/IEC 15408:2009 describes the IT security evaluation of a technology product. By the ISO/IEC 15408:2009, security requirements are used to evaluate the security of a product or system. The security requirements are divided into two groups: security functional and security assurance components. The functional components describe the requirements for the system. These security requirements are described by protection profiles (PPs) and security targets (STs). A protection profile is a set of implementation-independent security requirements, aiming to express IT security needs in general. A Security Target (ST) is a set of security requirements specifying the functional and assurance security measures for a target of evaluation (e.g. a product). The security assurance components, subdivided into classes, families, components and elements, help to verify whether the functional requirements were implemented correctly and securely. Security assurance components can be used to express PPs’ and STs’ requirements, and to evaluate them. Security assurance components describe requirements with regard to the security of a system. An assessment according to ISO/IEC 15408 can only be conducted by authorised entities. The CC consists of three main parts (see CC, 2006, p.12):

Part 1 is the introduction to the CC and defines general concepts and principles of IT security evaluation. It presents constructs for expressing IT security objectives,

for selecting and defining IT security requirements, and for writing high-level specifications for products and systems.

Part 2 is about security functional requirements as a way of expressing the functional requirements for the target of evaluation.

Part 3 is about security assurance requirements as a way of expressing the assurance requirements for the target of evaluation. Part 3 also defines evaluation criteria for protection files (PPs) and security targets (STs) and presents evaluation assurance levels for the assurance rating of the target of evaluation.

3.1.2.Risk assessment methods

In this section, information security assessment methods are presented, which have become best practices.

IT Grundschutz

The ‘IT Grundschutz’ or baseline protection manual (BSI, 2008), issued by the German Federal Office for Information Security (BSI - Bundesamt für Sicherheit in der Informationstechnik), contains a set of implementation guidelines, basic protection measures and guidance on system configuration. The baseline protection manual consists of standards, catalogues and tools to support information security. The following standards are included:

- BSI-Standard 100-1: Information Security Management Systems (ISMS)

  This defines general requirements for ISMS and is compatible with ISO/IEC 27001 (ISO, 2005d). It provides an easy and systematic introduction and instructions on how to meet the requirements of ISO/IEC with IT baseline protection.

- BSI Standard 100-2 IT-baseline protection methodology

This standard describes, step-by-step, how an information security management system can be built and operated in practice. The establishment of organisational structures for information security, and for security management activities, is an important issue. It provides detailed guidance on how a security policy can be created in practice, how appropriate security measures can be selected and what to consider when implementing the security concept.

- BSI Standard 100-3: Risk Analysis based on baseline protection

  The IT baseline protection catalogues contain standard security measures in the areas of organisation, personnel, infrastructure and technology. These measures are generally reasonable and adequate for the protection of typical business processes and information networks. This standard describes risk analysis on the basis of IT baseline protection.

- BSI Standard 100-4: Business Continuity Management

  This standard defines a systematic approach to build a continuous management process in a government organisation, or business, to ensure continuity of business operations.

In the “IT Baseline Protection Manual” standard, security measures for typical business processes, applications and IT systems are proposed. The aim is to provide adequate protection for all of an institution’s information. The standard contains a brief description of the considered assets, procedures and IT systems, and an overview of security concerns and safeguards. Through the application of security measures for a system described in the standard, a proper security level can be achieved at the organisation.

Standard of Good Practice

The “Standard of Good Practice” for information security from the Information Security Forum (ISF) was designed to help any organisation - irrespective of market sector, size or structure - to keep the business risks associated with its information systems within acceptable limits (ISF, 2005). The standard covers five major areas: security management, critical business applications, computer installations, networks and system development. In each area, further subareas are defined, which are then subdivided into sections. For each section, the corresponding principles and objectives are set, all the while describing what needs to be done and why with regard to information security. According to the ISF, the standard can be used to improve the level of security in an organisation in a number of ways: by assessing the performance of information security, by supporting security audits/reviews, and by checking compliance. The ISF standard claims to be the international benchmark on information security.

CCTA Risk Analysis and Management Method (CRAMM)

CRAMM was developed by the British government organisation, Central Communication and Telecommunication Agency (CCTA), which has since been renamed the Office of Government Commerce (OGC) (CCTA, 1987). CRAMM has three stages: identifying the scope of review, assessing threats and vulnerabilities and proposing countermeasures for risk. In the first stage, physical assets are determined and valued by “what if” questions. Secondly, assets are grouped and threat/vulnerability questionnaires performed. The responses to the questionnaires are scored and used to determine the level of risk. In stage three, countermeasures are proposed based on a list of safeguards. CRAMM provides a framework to calculate risks from asset values and vulnerabilities. The idea is that

the potential damage of an event can be identified by the value of the asset. The event is assessed on the likelihood and impact based on the three categories: integrity, confidentiality and availability. The necessary data for the assessment is collected via interviews.

Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) (Alberts et al., 2003), developed by the Carnegie Mellon Software Engineering Institute (SEI), is a framework to identify and manage information security risks. The assessment has three major phases: building security requirements, identifying infrastructure vulnerabilities and determining a security risk management strategy. Assets and risks are identified with structured interviews.

OCTAVE focuses on organisational risk and security practices rather than on specific technology or system evaluations. In the first phase, the critical assets of the organisation are identified by business and IT personnel, along with the current measures in place to protect these assets, security requirements and threats. Then, the related information technology components of the assets are identified and evaluated as to whether they are vulnerable to attacks. Finally, the risks to the critical assets of the organisation are identified, whereafter strategies and plans for mitigation are developed. OCTAVE uses security requirements to determine how an information asset is to be protected. Security requirements for confidentiality, integrity and availability are described verbally for critical assets and used for evaluation purposes. The phases of the OCTAVE approach are shown in Figure 3-1.

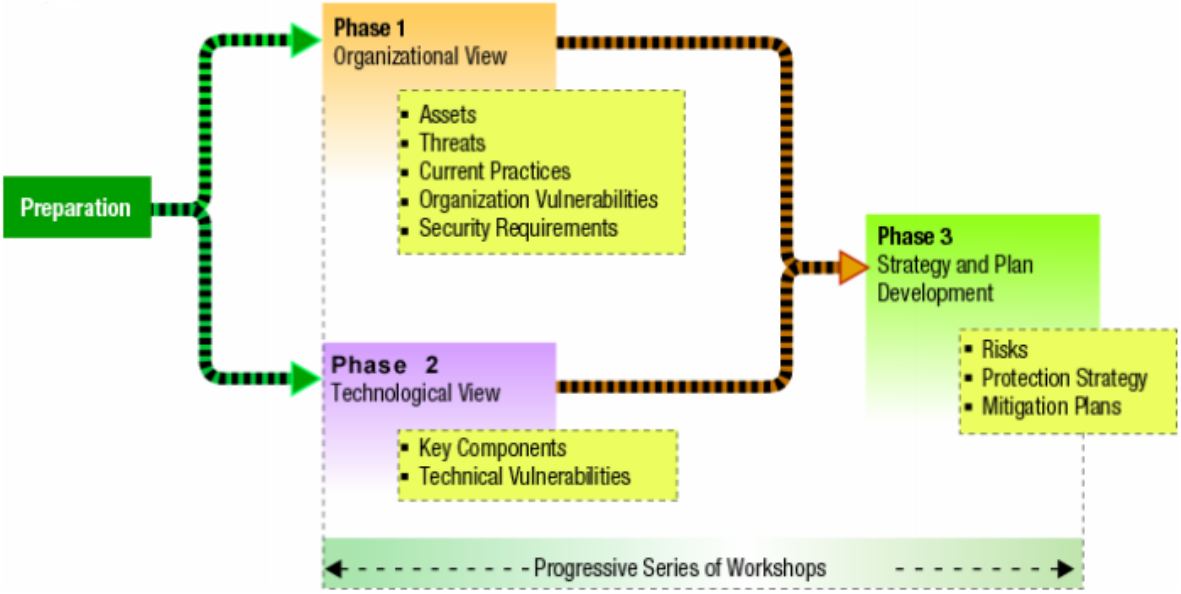


Figure 3-1 Octave phases from Alberts et al. (2003)

OCTAVE Allegro

OCTAVE Allegro (Caralli et al., 2007), developed by the Carnegie Mellon Software Engineering Institute (SEI), is a streamlined and fine-tuned version of the OCTAVE framework; it is said to be improved in terms of ease of use, resource requirements, risk results and compliance requirements. The goal of OCTAVE Allegro is to produce more robust results without extensive risk assessment knowledge and resource requirements. The focus of OCTAVE Allegro is on information assets and the context in which the information is used. OCTAVE Allegro consists of four phases and eight steps. These phases are as follows, and as shown in Figure 3-2:

- Phase 1 - develop risk measurement criteria. Here, a qualitative set of measures has to be defined against the risks and evaluated.

- Phase 2 - create a profile for each critical information asset. The most important assets are noted, as well as technical containers, physical locations and people.
- Phase 3 - identify threats to each information asset. These areas of concern are then expanded into threat scenarios (situations where the information asset can be compromised).
- Phase 4 - identify and analyse risks to information assets and develop mitigation measures. The threat scenarios created in phase 4 are evaluated, and the consequences are determined and rated against the measurement criteria of phase 1. For risks that were evaluated as 'high', an appropriate mitigation approach is defined.

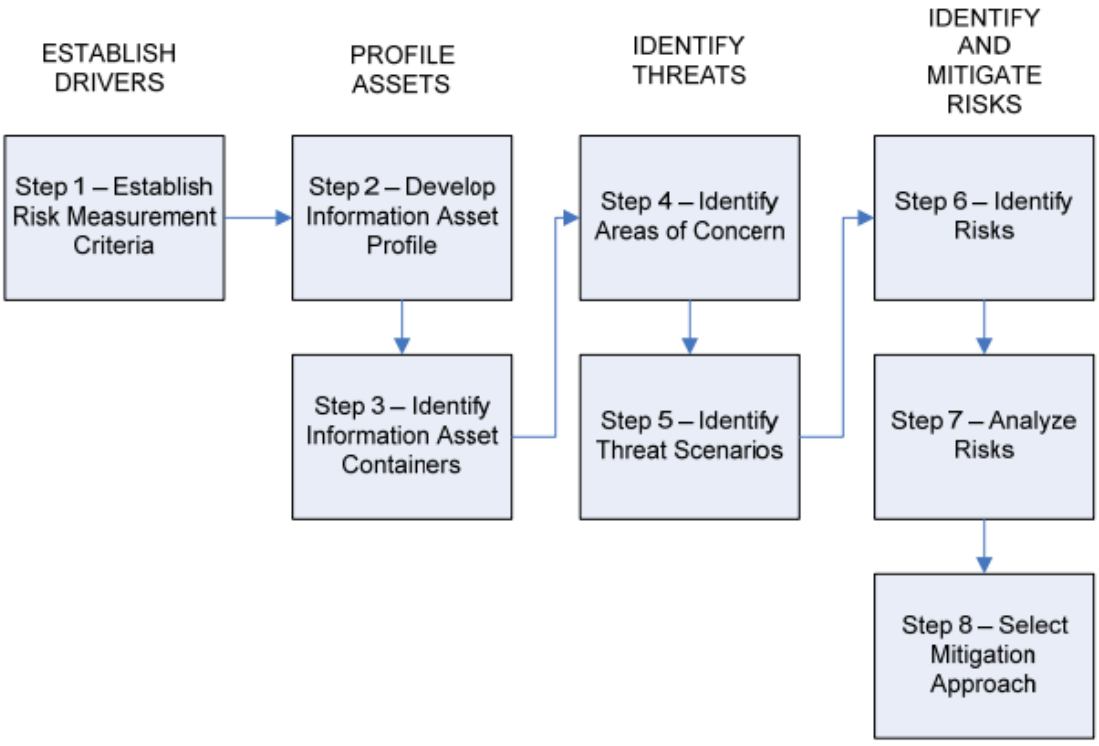


Figure 3-2 OCTAVE allegro from Caralli et al. (2007)

Control Objectives for Information and Related Technology (COBIT)

COBIT version 4.1 (ITGI, 2007) is a control framework for IT governance to link business goals with IT goals and the effective management of IT. The framework consists of 34 processes in four different domains, namely: plan and organise, acquire and implement, deliver and support, and monitor and evaluate. Within each domain, processes are defined with corresponding control objectives and controls, which can then be used to evaluate the current situation in an organisation. The adherence to these defined controls should provide assurance that business objectives will be achieved and undesired events will be detected, prevented or corrected. For each COBIT process, key goals and metrics are provided to measure the performance and outcome deviations. Figure 3-3 shows the structure of a security control objective description in COBIT. At the top right of the figure, the domain is shown (e.g. Plan and Organise). On the left, the process, requirements and control objectives and metrics are described for the process in a kind of waterfall. At the top left, the information criteria to be followed are defined. At the lower right, the IT resources for achieving the business requirement are indicated.

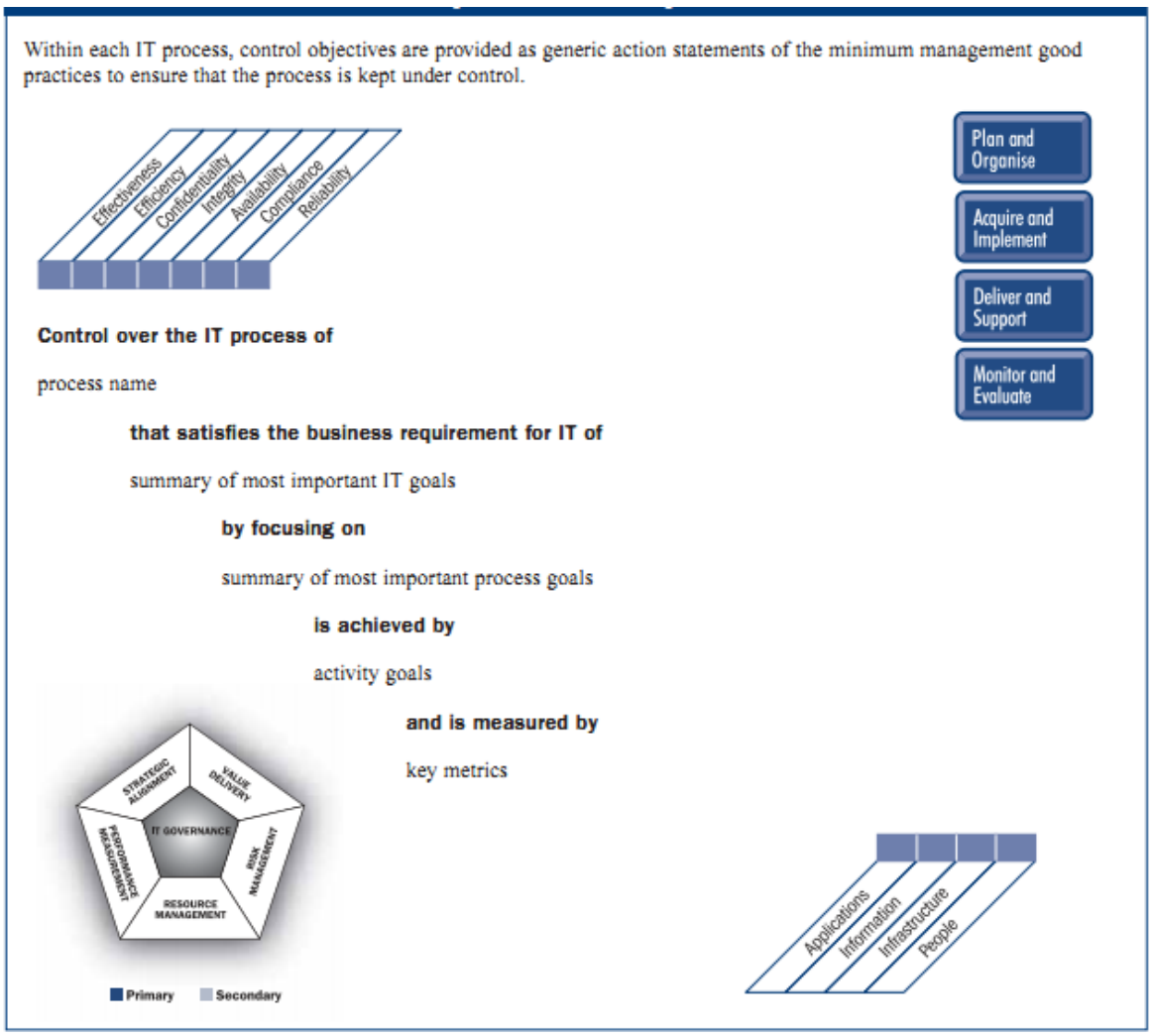


Figure 3-3 COBIT process description from ITGI (2007)

CORAS

Within the CORAS project (Stølen et al., 2002) - a research and technology project funded by the EU (2001 - 2003) - a framework for risk assessment of security-critical systems was developed. The CORAS risk management process is mainly based on the risk management standard AS/NZS 4360 (ASNZ, 2004) and the information security standard ISO/EC 17799 (ISO, 2005c). CORAS has five main phases based on AS/NZS 4360: (1) identify context; (2) identify risks; (3) analyse risks; (4) evaluate risks; and (5) treat risks. Each is supported by models that should be constructed, as well as advice on how they should be expressed. At

every phase, different methods of risk analysis are adapted, extended or combined - for example, Event-Tree-Analysis, Markov, HazOp and FMECA are all used. The platform uses open-source technologies like Java, XML and UML profiles for a model-based risk analysis of security-critical systems. Figure 3-4 shows the symbols for model elements which can be used to model risks.

Figure 3-4 CORAS modelling language elements from Braber et al. (2007)

Information Security Management Maturity Model (ISM3)

The Information Security Management Maturity model (ISM3, 2007) is a framework for security management developed by an industry consortium. The framework describes common information security processes with underlying performance targets and metrics. The ISM3 handbook describes the security processes for each of the four categories - general, strategic management, tactical management and operational management - and the rationale behind choosing these processes. For each of those described, parameters such as output, input, activities and responsibilities are defined. These can be used to evaluate the current security maturity of the organisation and form the maturity level rating.

NIST Risk Management Guide SP 800-30

The National Institute of Standards and Technology (NIST) Risk Management Guide for Information Technology Systems Special Publication (SP) 800-30 (Stoneburner et al., 2002b) provides a foundation for developing an effective risk management programme. NIST, founded in 1901, is an agency of the U.S. Department of Commerce. Its goal is to promote competitiveness by advancing measurement science, standards and technology. The main focuses of NIST SP 800-30 are the risk assessment and risk mitigation processes. Therefore the guideline, through several steps, describes how to identify, determine, mitigate and document risks. For each process step, the inputs, outputs, and the activities to be performed are defined. The activities primarily describe the risk assessment procedure, suggesting how to perform these activities. The risk assessment has nine steps as shown in Figure 3-5:

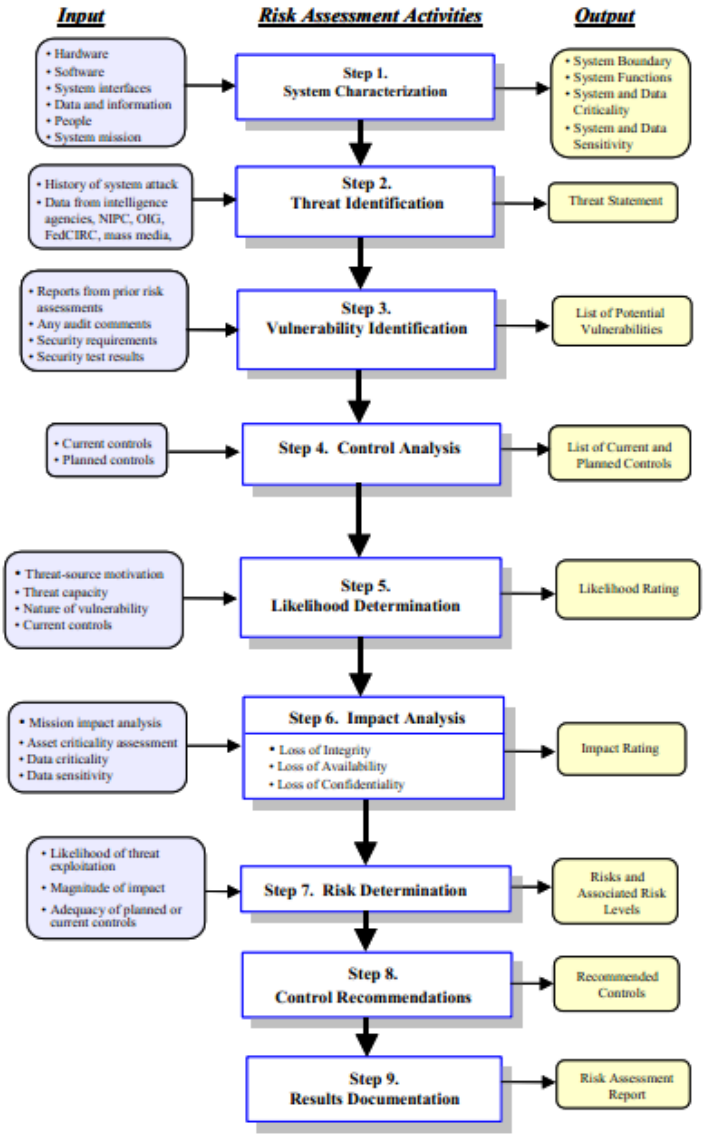


Figure 3-5 NIST risk assessment steps from Stoneburner et al. (2002b)

IT Infrastructure Library (ITIL)

The IT Infrastructure Library (ITIL) (CCTA, 2007) is a set of best practice processes and concepts published by the UK Office of Government and Commerce (OGC). The main focus of ITIL is on IT service management; it provides descriptions of processes to help implement and manage IT services. The two key building blocks of ITIL (version 2) are service delivery and service support, the former of which is about the proactive management of the service

provided - it contains sub-processes such as capacity management, availability management and continuity management. Service support, meanwhile, concentrates on the user and the support of business functions. Within service support, there are also sub-processes such as service desks, problem management, change management and configuration management. Another separate aspect of ITIL is security management, where the organisational involvement of information security is described. The content of this set of best practice processes is mainly based on the ISO 17799 (ISO, 2005c) standard, and describes how service support and delivery are affected by security management. ITIL version 3 is a further development and is now based on a life-cycle approach. This life-cycle approach is reflected by new building blocks such as service strategy, design, transition, operation and improvement.

Expression of Needs and Identification of Security Objectives (EBIOS)

EBIOS (ANSSI, 2010b) stands for “Expression des besoins et identification des objectifs de sécurité” (French). EBIOS was published in 1995 and developed by the DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), the French Ministry of Defense. The most recent version was published in June 2010. The EBIOS method consists of a set of principles - analysis of the context, expression of security needs, threat study, identification of security objectives and security requirements - as shown in Figure 3-6.

Firstly, the context has to be analysed with regard to general requirements, the owner of systems as well as further information about the assessment. Then, the security needs and the threats are identified in two separate activities. Security needs are expressed in terms of availability, integrity and confidentiality by the system users. Threats are identified by spotting attack methods and the

corresponding vulnerabilities of the system. Within the next activity, “identification of security objectives”, risks are determined by combining threats and their impact on security needs. Security objectives of the system are evaluated with regard to the risk identified, and whether there are any conflicts between them. In the final activity, the necessary and sufficient security requirements are determined and the security controls contributing to the requirements are checked. Any residual risks are shown by comparing the security requirements and controls to the risks.

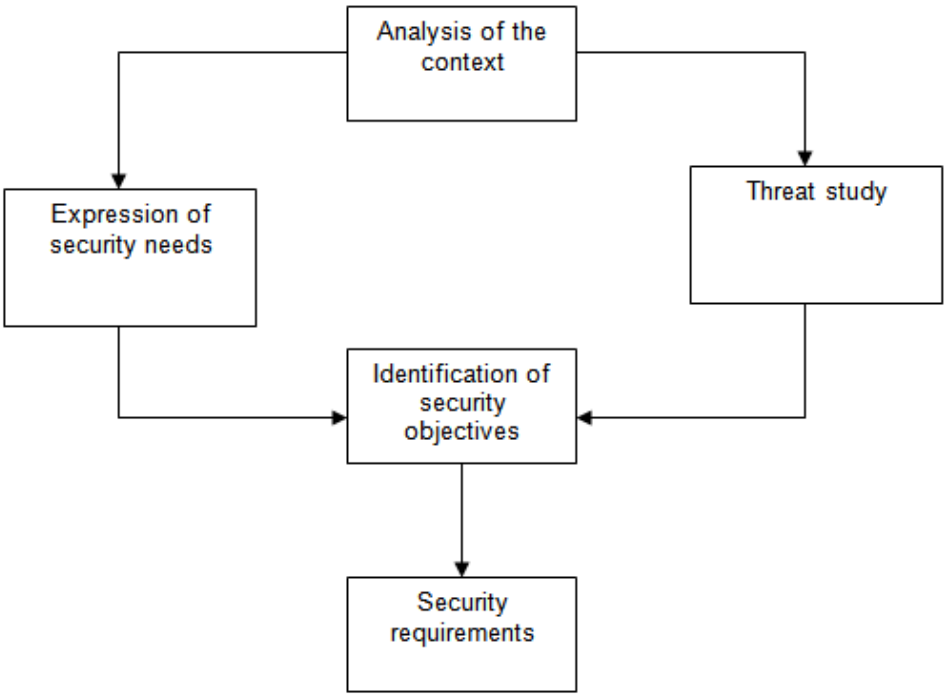


Figure 3-6 EBIOS set of principles from ANSSI (2010b)

Harmonised Risk Analysis Method (MEHARI)

MEHARI (Méthode Harmonisée d'Analyse de Risques — Harmonised Risk Analysis Method) (CLUSIF, 2010) is a risk assessment method developed by CLUSIF (Club for the Security of Information in France, or Club de la Sécurité de l'Information Français). MEHARI was, like EBIOS, last updated in 2010. The MEHARI risk assessment is based on a knowledge base that has to be developed

before the risk assessment. The knowledge base contains assets and potential damages to these assets (including vulnerabilities and threats), which form the basis for the risk scenarios (events or threats impacting upon an asset, with a rating of likeliness of any impact for the company). Based on the risk scenarios that were determined, the risks and their corresponding parameters are evaluated, bearing in mind the likelihood and impact of the risk. Figure 3-7 shows the knowledge base creation, the assessment process and their subsequent activities.

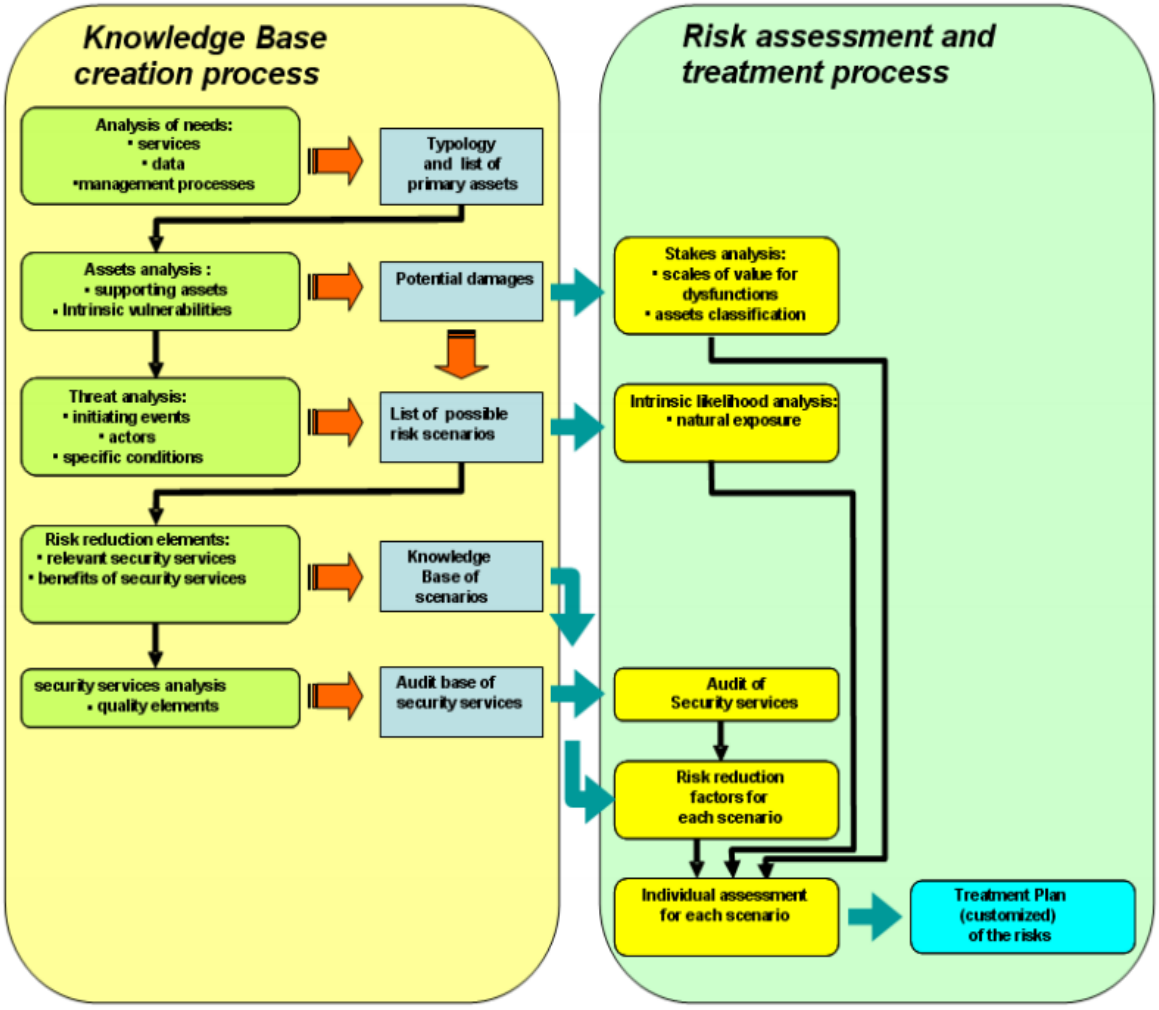


Figure 3-7 MEHARI steps of risk evaluation from CLUSIF (2010)

Generally Accepted Information Security Principles (GAISP)

GAISP (ISSA, 2004) - the Generally Accepted Information Security Principles - contains a set of security principles that were proven and accepted in practice. GAISP is published by the Information Systems Security Association (ISSA) but was originally drafted by the Information Security Forum (ISF). Its principles are subdivided into pervasive, broad functional, and detailed. Pervasive principles provide general governance-level guidance to establish and maintain the security of information. The broad functional principles describe what to do at a high level of the pervasive principles, allowing a definition of the basic units of those principles. The detailed principles describe the methods of achieving the broad functional principles, with reference to the specific environment and current technology. In this publication, the description of the broad functional principles, e.g. education and awareness, accountability, takes up most space.

Livermore Risk Analysis Methodology (LRAM)

The Livermore Risk Analysis Methodology (LRAM) - developed by Guarro et al. (1987) at the Lawrence Livermore National Laboratory - uses risk scenarios, which they call “risk elements”. Firstly, in the information gathering phase, the data of systems are identified. Then risk scenarios are created containing the data systems, determining their monetary value, loss consequences, and possible threats. The evaluation of the risk scenario is conducted, both with no controls, and all controls applied, in order to determine the level of security. Figure 3-8 shows the phases of LRAM - planning, risk analysis and management decision support - and the stages of each phase, ending with the prioritisation and selection of the proposed control sets.

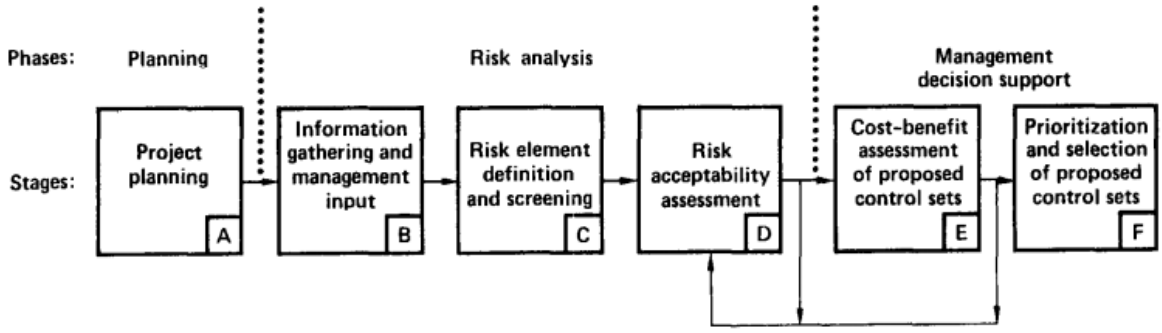


Figure 3-8 LRAM process diagram from Guarro (1987)

Security Process Maturity Models

A process maturity model is a method for assessing implemented processes including the process objective, best practices and improvements over time. The objective of a process maturity evaluation is to determine any improvements over time, to compare with peers or best practices, and to improve the performance with regard to cost, schedule, productivity, quality and customer satisfaction, among others (Paulk et al., 1993). Mostly five levels are defined to measure the process maturity (Woodhouse, 2008) and how the process is conducted and controlled. In the following, only the two predominant maturity models (CMM and SPICE according to Wendler (2012)) are presented.

Capability Maturity Model Integration (CMMI)

The first process maturity framework to be designed was the capability maturity model (CMM) for the software engineering institute (SEI-CMM) in 1987 (Paulk et al., 1993). The initial SEI-CMM model was applied to different domains, and therefore variants were developed, such as the capability maturity model for software (SW-CMM), the software acquisition capability maturity model (SA-CMM)

and the people capability maturity model practices (P-CMM). The SEI-CMMI is a further development of the SEI-CMM, and provides a set of 16 core areas to improve processes. The objective of CMMI is to provide guidance to develop or improve processes around the business objectives of an organisation. CMMI covers areas like development, acquisition and services.

Software Process Improvement and Capability Determination framework (SPICE)

The Software Process Improvement and Capability Determination framework, called SPICE (ISO 15504) (ISO, 2004a), is an assessment method developed by the International Organisation of Standardisation (ISO) for the evaluation of products and services. SPICE is mainly used in the software engineering domain. The assessment is based on a process reference model defined in ISO 12207 (ISO, 2005a), and consists of primary (e.g. acquisition, engineering, and operation), support and operational processes (e.g. management, process improvement) as well as the maturity levels defined in the ISO 15504.

3.2. State of the art

In the following the information security risk assessment approaches developed by researchers from different fields in the computing area are presented. Approaches from information security which use security requirements and business process models for risk assessments, software engineering and business process management are presented and organised by area. The identified information security risk assessment approaches in these areas were examined, with specific regard to how security requirements are used and vulnerabilities determined.

3.2.1. Risk assessments for organisations

In the following, the information security approaches are presented that use *business processes*, *organisational models* or *security requirements* for the assessment of information security risks within an organisation.

Business processes

In early risk assessment approaches, the idea of using business processes was introduced. Rainer et al. (1991) were among the first to align qualitative and quantitative risk analysis methods with the value chain of a company to determine risks based on assets. The value chain was used to enumerate critical business activities and IT components, as well as the linkage between them.

In 1996, Halliday et al. (1996) proposed the consideration of business issues, instead of comparing vulnerability checklist against systems. They suggest conducting the risk analysis on critical business processes of the organisation, based upon the continuity and availability of business operations. They use risk scenarios - defined as “undesirable situations” - where risks are classified based on their primary effects on confidentiality, integrity and availability, as well as their probability and potential impact. The risk scenarios are ranked and countermeasures proposed for high risks.

Suh and Han (2003) proposed an IS risk analysis method on a functional business model. A business function is defined as a business activity that supports one aspect of the organisation. Business objectives and their relative relevance are determined for functions and sub-functions. The Analytic Hierarchy Process (AHP) is used on the functions to evaluate the criticality of risks for operation. This

approach considers income loss, replacement costs and the importance of business functions, and is based on business functions (a process model is not used). It assumes that assets contribute directly to the business objectives.

Neubauer et al. (2005) proposed to connect business processes with IT processes. They compare the unavailability costs of core business processes with the IT security costs of different security levels, in order to determine the most cost-efficient solution. Security levels to be achieved are used to evaluate the cost benefit for IT security.

Khanmohammadi and Houmb (2010) centre on business goals, and the processes that support them. They identify the relevant business processes for business objectives and the control processes responsible for security. Then, vulnerabilities are identified by best practices or security bulletins and assigned to specific control processes. The ability of the control processes to protect against vulnerabilities is measured. To calculate the risk for a process, the exposure degrees of a vulnerability - as well as threat frequency and impact - are used. The difference of their approach is that vulnerability and risks are determined for processes, rather than for single assets.

Organisational models/frameworks

The TOPM (Target Optimum Portfolio Approach) approach, developed by Badenhorst and Eloff (1994), is an approach based on a life-cycle model with the main objective to optimise the risk management process. Matrix theory, transaction routes, and different domains - organisation, technology, people and systems - are considered to determine risks.

Bandyopadhyay et al. (1999) proposed a framework for IT risk management which offers managers a comprehensive view of their risk situation. This involved considering different levels (inter-organisational, organisational, and application) in risk identification, analysis, reduction and monitoring, and their work thus focuses on the linkage of the risk management processes at inter-organisational, organisational, and application levels.

Innerhofer–Oberperfler and Breu (2006) use an enterprise model that combines and reflects the organisational unit, the business processes and the applications and systems used. They use security objectives (for the process) and security requirements (for sub-processes and activities) to define the required security. The enterprise model with its dependencies is then evaluated, considering threats, vulnerabilities and the defined security requirements. The impact and probability of the risk is then evaluated on a qualitative scale.

Sun et al. (2006) use the Dempster-Shafer Theory of Belief Functions to model uncertainties involved in the information security assessment process. The focus of their approach is to model and consider uncertainties that are present in every risk assessment. Therefore, this theory is used to express the degree of belief in the evidence that is available for either the presence or absence of risk. The model uses evidences and assertions and links them. For each assertion, the degree of belief is calculated based on the evidence.

Security requirements/metrics

Information technology risks of a company are determined not only by events or vulnerabilities of a system, but also by the required security from a business perspective, regulatory or statutory requirements and applicable laws (Gerber and von Solms, 2001; ISO, 2005c). Therefore, security requirements of the company should be specified to determine risks not only by technical vulnerabilities.

The approach of Thoben (1997) with regard to an IT system risk analysis specifies security requirements (static and procedural) for IT system elements based on a threat and vulnerability examination. Threats, vulnerabilities and their consequences are modelled and then compared against the system configuration, with regard to the security requirement. Then, the validity of the security requirement is determined. The focus of this work is on the modelling and checking of security requirements with a risk analysis.

Gerber et al. (2001) suggest specifying security requirements by security concerns and their intensity level (level of protection needed). In their work, they use a qualitative classification scheme - a matrix of impact and business relevance - for the rating of each security. However, their work stops at the identification of security requirements.

Chung et al. (2005) propose security risk vectors for evaluating assets quantitatively. Therefore for servers, application and data, the security objectives' confidentiality, integrity and availability are rated by a metric value. Then a vector value is calculated for each asset, as well as for those related to it. With the

security vector value, a comparison of the criticality and importance of an asset can be determined. The focus of their work is on asset evaluation.

Manadhata and Wing (2005) present a metric - the attack surface - that expresses the security of a system in comparison to different versions of the same system. The metric is based on the “attack surface”, i.e., the system’s attackability, along three dimensions: method, data and channel. In comparison to other security metrics, such as number of bugs found (code-level) and number of times a system version is mentioned in CERT advisories (system-level), their proposed metric lies between both - on the design-level of a system. The attack surface is expressed as a triple value; it bears in mind the attackability of methods, data and channel of the system.

3.2.2. Risk assessment in software engineering

In software engineering, it is widely acknowledged that one should address security from the beginning. This is because reacting to security issues is time-consuming and expensive. Therefore researchers in software engineering have proposed *modelling notations and frameworks* to consider security already in the system development phase. *Modelling notations* are used to capture information, make it explicit, and act as a repository of knowledge. *Frameworks* are used to derive and analyse security requirements. Security requirements describe the necessary security for systems to protect against threats. Below, *modelling notations* and *frameworks* that have been developed are presented.

Modelling notations

Several modelling notations have been developed for security aspects. One can distinguish between two categories: the *modelling of attacks and vulnerabilities* and *capturing countermeasures and security requirements*. Modelling notations are used for analysis and visualisation of information and requirements.

For *attack and vulnerability modelling*, methods like misuse cases (Sindre and Opdahl, 2005), abuse cases (McDermott and Fox, 1999) or the malicious actor in the enhanced i* framework (Liu et al., 2002) have been developed to describe unwanted behaviour. A misuse case is the opposite of a use case, where a use case describes the function the system should perform (Cockburn, 2001). Therefore, it can be said that a misuse case describes the function a system should not allow. The misuse case can be used in the representation of relevant information and the elicitation of security requirements. Abuse cases describe the interaction between a system and one or more actors that result in harm to the system (McDermott and Fox, 1999). They are specified in natural language or in a tree and modelled in the Unified Modeling Language (UML). Abuse cases can be helpful in the requirements, design and testing phases of a system.

In the work of Liu et al. (2002), they use an actor in the i* framework to determine vulnerabilities, by assuming malicious intentions of the actor. Actor dependency analysis is used to identify attackers and threats. The i* framework (Yu, 1997) was developed to model and reason about the organisation and information systems; it consists of the strategic dependency and strategic rationale model and supports goal-modelling and analysis of requirements.

For identifying vulnerabilities and specifying attacks, attack trees (Schneier, 1999) and attack graphs (Phillips and Swiler, 1998) have been developed. Attack trees describe the different ways in which a system can be attacked. The root of the tree represents the goal of the attack, while leaves and branches describe the ways to achieve the goal. Attack graphs are based on attack templates, where the conditions and activities of known attacks are described. Threat modelling (Mockel and Abdallah, 2010) is similar to attack modelling but focuses instead on threats and their mitigation. Threat modelling is about identifying threats for system components and mitigating them by proposing security concepts. Threat modelling starts by defining security objectives, then decomposes the system into functional areas and data flows and then identifies threats by threat categories and their effect to the decomposed system. After that, mitigation concepts are elaborated to secure the system. For threat modelling, often data flow diagrams (DFD) and Unified Modeling Language (UML) are used to represent data flows, system components actors and actions.

In addition, problem frames (Jackson, 1999) have been used to compose threat descriptions (Haley et al., 2004). With problem frames, larger problems are decomposed into smaller ones, describing the interaction of domains with the real world. Concerns surrounding assets or objects of the problem context are used to specify threats.

For the *modelling of security relevant information, countermeasures and security requirements* methods, like UMLsec (Jürjens, 2005), secure TROPOS (Giorgini and Mouratidis, 2005) or the work of Matulevicius et al. (2008) can be used. These methods were developed to capture security specific concepts to protect against

malicious actions. UMLsec (Jürjens, 2000; 2002; 2005; Jürjens and Wimmel, 2005) is an extension to UML, used for integrating security related information into UML diagrams. With UMLsec, one can express security relevant information in UML and then use that information for the formal evaluation of design and specification. Secure TROPOS (Giorgini and Mouratidis, 2005) is an extension to TROPOS used for considering security issues during the software development process. TROPOS is a software development method that uses the concept of agents to model and analyse security requirements and their software design. In secure TROPOS, the concept of constraints was introduced and extended, with regard to security. Constraints are restrictions regarding actions or achieving goals, and have been defined as a new model element. Matulevicius et al. (2008) align Secure TROPOS to the security risk management process. They suggest a number of improvements for Secure TROPOS to model business assets, IS assets, threats and security requirements. With all these notations, specific security aspects such as attacks, malicious actions, vulnerabilities and countermeasures can be modelled.

Frameworks

Several security requirement frameworks were proposed for eliciting, modelling and analysing security requirements. The main objective of these frameworks is to provide a list of feasible security requirements for “good enough” security for a system. The foundations of developed frameworks used are mostly goals or anti-goals, trust or trust assumptions, and threats and vulnerabilities. Frameworks such as the i* framework (Yu, 1997), KAOS (van Lamsweerde and Letier, 2000), SeDAn (Chivers and Fletcher, 2005), TROPOS (Giunchiglia et al., 2002) or the Security Engineering Framework (Haley et al., 2008) have been developed. They

should help to identify security requirements and evaluate the system design satisfying these security requirements. The i* framework (Yu, 1997) was developed to model and reason about the organisation and information systems. It consists of the strategic dependency (SD) and strategic rationale model (SR). The SD model describes dependencies between actors in an organisation; the SR model focuses on stakeholder interests and concerns, and how they might be addressed by a system configuration. The KAOS (Knowledge Acquisition in Automated Specification) approach is about identifying goals and refining them into system requirements and objects. A KAOS model includes a goal, object, agent and operation model. The goal model describes the system-to-be, the object model describes the objects of the system, the agent model the responsibilities of agents for goals, and the operation model the interaction of objects. SeDAn (Chivers and Fletcher, 2005) uses an information flow graph to determine whether there is a path for an attacker to information assets. Information asset flows are modelled as services, and an attack model used to determine exploitable paths. TROPOS (Giunchiglia et al., 2002) is a methodology which helps to describe the organisational environment of a system, as well as the system itself. TROPOS is based on the i* framework using the concepts of actors, positions, goals and dependencies. The framework of Haley et al. (2008) is about security requirement elicitation and analysis. Assets are identified; security goals and requirements are determined. Satisfaction arguments are then used to validate the security requirements.

Other more practitioner-oriented methods for security requirement elicitation are SQUARE, SIREN and CLASP. The SQUARE (Security Quality Requirements Engineering) (Toval et al., 2002) methodology was first published in 1995. It is

primarily about eliciting, categorising, and prioritising security requirements for systems. The elicitation of security requirements is based on vulnerabilities and risks of artefacts having security goals - identified beforehand. SIREN (SImple REuse of software requiremeNts) (Toval et al., 2002) is a requirement-reuse approach where requirements are stored in a repository, drafted by applying Magerit (MAGERIT, 2006) - a risk assessment approach - and reused for system development. CLASP (Comprehensive, Lightweight Application Security Process) (Viega, 2005) is a software development method to address security based on best practices. CLASP claims to be the first structured method to build security requirements for systems, and comprises a set of process activities that should be conducted before and during the development process by those involved.

3.2.3. Risk assessment in business process management

Business process management is about the workflows and processes of an organisation. In the following, approaches of the workflow management and business process modelling field are presented, considering information security risk (assessment).

In the workflow management field, security requirements are used to design/verify workflow systems or business processes. A business process model can be described as a set of activities to reach an objective. “A business process is widely defined as a structured flow of activities which supports business goals, and is facilitated by data and resources” (zur Muehlen, 2005, p.3). These activities are performed by actors using resources such as systems, materials or information and may be dependent on other activities. Workflow management builds on the business process models and implements the defined processes with regard to

automated execution. Workflow management includes the execution, organisation, controlling and monitoring of work sequences (Janssen, 1998). Workflow management is a level between the process model and the technical implementation with systems. There are some approaches which focus on creating secure business processes or workflows based on security. Security requirements are defined for business process activities or workflows that have to be adhered to - in so much as having a secure process/system. Backes et al. (2003) proposes a guideline to integrate security requirements into the business process modelling, Atluri (2001) proposes to consider security requirements for workflow systems, and Herrmann and Pernul (1998) propose enforcement of security requirements in workflow management. Other approaches do also attempt to analyse security requirements of business processes (Roehrig, 2003; Roehrig and Knorr, 2004), and question which security measures should be implemented. Other researchers attempt to verify the consistency of workflow implementations against security policies (Ribeiro and Guedes, 1999). The aforementioned approaches focus on the creation or analysis of security requirements within business processes or workflows to define or implement secure processes. However, these approaches omit an assessment component and do not consider already implemented security measures.

Approaches in the business process modelling field use business process models to represent and analyse risks (including information technology risks). Zur Muehlen (2005) proposes a framework of four interrelated risk models - namely a risk structure, risk goal, risk state and extended Event-driven Process Chain (EPC) model (a flowchart used for business process modelling) - to present risks of a business process. With these four models, risks of a business process are

intended to be captured and modelled, for the purpose of risk management. The proposed risk models of Zur Muehlen should help to document process-related risks and increase risk-awareness.

In another paper of Zur Muehlen and Ting-Yi (zur Muehlen and Ho, 2005) the authors provide an overview of the risks of business process management projects with regard to the life-cycle. For each of the different phases of the project life-cycle - analysis, design, implementation, enactment, monitoring and evaluation - risk factors were identified. These risk factors describe risks closely related to the life-cycle process, and the work is focused on business process management projects and risk factors for such project phases.

Neiger et al. (2006) further develop and promote the idea of Zur Muehlen (2005) by determining risks with business process models. They propose a four-step approach for risk identification in business processes: to decompose business objectives, to identify risks by value-focused thinking, to determine alternative process configurations and then to compare alternative processes. Risks are determined by business values and fundamental business objectives to be achieved by the process. Then, alternatives for the business process and business objectives are considered and compared, in order to reduce the identified risk.

Lambert et al. (2006) enhanced the business process notation, Integration Definition (IDEF), with the value “sources of risk” being used to describe risks at the activity level. Identified risks are modelled and linked to the corresponding process activities, thus helping to visualise risks in the process. The process sequence and the risks of the process activities can then be analysed to allocate

resources and prioritise activities accordingly, with regard to the risks and process objectives.

Rodriguez et al. (2007) extend the Business Process Modelling Notation (BPMN) to specify security requirements within business process models. The security requirements consist of five attributes - non-reputation, attack harm detection, integrity, privacy and access control. The security requirements are indicated as locks over message flows, roles or data. This approach is essentially an extension of the BPMN to model security requirements in business processes.

Jallow et al. (2007) propose a framework for assessing operational risk in business processes on the basis of time, cost and performance/quality relative to process activity level. They identify risk factors (events) of a process and determine their respective probabilities. With a triangular probability density function, they thus determine the overall impact on costs.

Herrmann and Herrmann (2006) use $MoSS_{BP}$ - a framework to specify security requirements and analyse business processes' fulfilment - and object-oriented security analysis in order to facilitate the automated realisation of business processes' security requirements. Security requirements are assigned to business processes. For each, corresponding security measures from a repository of safeguards that adhere to security requirements are proposed.

Islam et al. (2009) suggest a risk management approach based on vulnerability and criticality on an organisational level, mitigated at the business process stage. The i* framework out of the software engineering domain is used, looking at the

strategic relationships between process participants. Actors and their dependencies are modelled in i* and the actors' incoming/outgoing dependencies are used to indicate vulnerability and criticality. Monitoring of tasks of vulnerable actors is used to mitigate risk and then modelled in the business process. However, Islam et al. consider only actors; they do not assess systems or activities of processes.

3.3. Discussion on risk assessments

In this section, the current state of risk assessment methods in the different research fields within the computing area is reflected upon; how vulnerabilities are determined in these methods and whether an asset's security requirements are used for vulnerability identification are answered - firstly based on information security risk assessment methods for organisations which represent the majority and main research object, secondly on approaches in software engineering, and thirdly on approaches in business process modelling.

3.3.1. For organisations

Risk assessment approaches utilising business processes or business functions use, for example, annual loss expectancy (Suh and Han, 2003), loss of disruption (Neubauer et al., 2005) or business goals (Khanmohammadi and Houmb, 2010) to determine the criticality and importance of threats and vulnerabilities. With these approaches, the reasonable level of security and a risk estimate for assets within the value chain should be determined. But approaches that use business processes base their valuation of assets and risks on the impact of vulnerabilities in terms of losses or interruption of the business.

A few approaches use risk scenarios, defined as “undesirable situations”, like Mehari (CLUSIF, 2010) or LRAM (Guarro, 1987), to determine the risks faced by an organisation. A risk scenario comprises a threat, frequency and impact and is constructed by determining what could befall a system. The risk scenario is then evaluated against the security control implementation with regard to its respective likelihood. Risks are then classified against security objectives - confidentiality, integrity and availability. Risk scenarios can be described and applied specifically to an organisation, but vulnerabilities are determined upfront, independently of the security control implementation and security needs. In addition, threat lists or security best practices are used for describing vulnerabilities and risk scenarios.

Some approaches propose frameworks or modelling for risk assessment. Sun et al. (2006) use the Dempster-Shafer Theory of Belief Functions to model uncertainty in risk assessments; Bandyopadhyay et al. (1999) consider the inter-organisational, organisational, and application level in the risk identification process; Badenhorst and Eloff’s (1994) approach is about risk management process optimisation based on a life-cycle model; and Thoben (1997) models security requirements for developing secure systems. In addition, metrics are proposed by researchers to evaluate assets quantitatively. For example, security risk vectors (Chung et al., 2005) are used for the ranking of risks; or the attack surface (Manadhata and Wing, 2005) for the comparison of different versions of a system. These approaches focus on optimising the risk assessment process and considering further information for risk valuation or the quantitative ranking of risk, while threat lists or security best practices are used for identifying vulnerabilities.

There are several approaches - COBIT (ITGI, 2007), ISF (ISF, 2005), Baseline protection manual (BSI, 2008), GAISP (ISSA, 2004), ISO/IEC 27002 (ISO, 2005e) - that all describe best practices of security solutions to be implemented, security principles to be applied and common threats and vulnerabilities. In CORAS (Stølen et al., 2002), structured brainstorming and security best practices are used to identify risks. Any identified threats and vulnerabilities are documented in a threat diagram supported by a modelling language. These approaches can be seen as knowledge bases, or security best practices, and can be used to determine vulnerabilities. However, the vulnerabilities and proposed security solutions used to identify vulnerabilities are unspecific to an organisation and name only universal procedures.

Security requirements were proposed (Gerber et al., 2001) for determining security controls with regard to the security needs of the business. In several approaches, security requirements for assets are defined and used to determine the criticality and impact of vulnerabilities, as well as for the selection of security solutions. But for vulnerability identification, knowledge bases or security best practices are still used. For example, Innerhofer-Oberperfler and Breu (2006, p. 9) state that, to identifying possible threats that can violate a security requirement, “existing security checklists or standards like the Baseline Protection Manual or EBIOS can be used”. In OCTAVE Allegro (Caralli et al., 2007), the risk identification begins with “brainstorming about possible conditions or situations that can threaten an organisation’s information asset” (Caralli et al., 2007, p.18). Then, threat scenarios are identified out of the brainstorming session or on the basis of a predefined threat tree. For each threat scenario, “how this threat would affect the security requirements that have been set for the information asset” is documented (Caralli

et al., 2007, p.59). In NIST 800-30 (Stoneburner et al., 2002b), vulnerability knowledge bases, system security testing and a security requirement checklist are used for vulnerability identification. The security checklist specifies high-level security criteria for IT systems using a knowledge base - for example, government regulation or security directives. The security requirements of this checklist can be described as the control objectives and can then be used to determine vulnerabilities of assets. This security requirement checklist is not specific to an asset, and how to apply the checklist is not further elaborated. In EBIOS (ANSSI, 2010a), threats and security requirements are identified and defined in two parallel process steps. Threats are identified based on attack methods on (and vulnerabilities of) systems. Then, threats and security requirements are combined to determine the impact on the security caused by the threat for identification. In the Common Criteria (CC, 2006), security requirements are used to evaluate a product or specification, and to provide assurance that it meets any requirements. But the CC is product-oriented, not IS-oriented, and therefore is not suitable for assessing the information security risks of a company.

Security risk assessment methods, like COBIT (ITGI, 2007) providing security objectives and a maturity assessment component, or ISM3 (ISM3, 2007) providing an information security management process model, are a mixture between a security maturity assessment and a security risk assessment - generally with particular emphasis on one of the two areas. A linkage between security maturity models and security risk assessment methodologies could be beneficial, as not only the current risks but also the capability of the organisation to react to risks or events are of interest. This benefit results from the fact that risks change over time due to underlying conditions (Kinney, 2003), the problem space (Jackson, 2007)

and environmental changes; therefore, security risk results should not be dependent on the point of time of the assessment. But current security maturity assessment approaches are checklist- and best practice-driven. This means that the assessor has to choose the security objectives or security controls that apply, unspecific to the organisation. Furthermore, these approaches miss an assessment component - how to determine the adherence of these security objectives, or how to determine any vulnerabilities.

To conclude, all the approaches and concepts used to identify vulnerabilities and risks are closely aligned to the definition of risk: occurrence of an event with a certain probability of causing an impact (a positive or negative one) (ISO, 2005c). The approaches start with the identification of events, threats and vulnerabilities or defining a scenario, and then determine probabilities and impacts, following risk management standards like AS/NZ 4360 (ASNZ, 2004). Security requirements are only used to determine the impact of vulnerabilities or as a justification for a risk - *not for identifying vulnerabilities or risks*. The few approaches that use security requirements for vulnerability identification use them as a generic checklist or do not specifically evaluate them with regard to the security functions applied at the organisation. For example, in NIST SP 800-30 (Stoneburner et al., 2002b) the security checklist is compiled by referring to government regulatory and security best practices, which does not reflect the specific asset's security needs. In Innerhofer-Oberperfler and Breu (2006) as well as OCTAVE Allegro (Caralli et al., 2007), threats and vulnerabilities are compared to security requirements and it is determined whether they have been violated, but they are not evaluated. Common Criteria (CC, 2006) specifies security requirements only for a product, not for an organisation, and therefore it is only suitable for the evaluation of a system.

To summarise, in all these risk assessment approaches, security requirements of information assets are not analysed to identify vulnerabilities with regard to the security functions implemented in the organisation. They concentrate on the presence of vulnerabilities, but not on determining whether security requirements - business security needs - are fulfilled and vulnerabilities absent. No analysis method or guidance is proposed for evaluating security requirements with regard to the current implementation to identify only (true positive) vulnerabilities.

3.3.2. In software engineering

The main focus of security requirement frameworks and modelling notations is on the design and development of a system. These approaches support (either partly or fully) the software engineering phases - early and/or late requirements; architectural and detailed design. The goal of these approaches is to identify, specify and verify security requirements for systems for the design and implementation of security functions. Within modelling notations, security aspects like attacks, malicious actions, vulnerabilities and countermeasures are modelled to determine “good enough” security for systems in the form of security requirements. The focus of modelling notations is on security issues that can occur through use or abuse of the system. The output of security requirement frameworks is a list of feasible requirements for a “good-enough” system's security against potential attacks. Security requirements are then evaluated, to examine whether a certain system design can satisfy the requirements.

Security requirement frameworks and modelling notations are helpful in the elicitation and modelling of security requirements, identifying countermeasures

and determining the security design, but they cannot identify and represent risk from an organisational risk management perspective. This is because these languages mostly lack of constructs for representing risks (Dubois et al., 2010) and make no use of a risk-based approach (Mayer, 2009). Furthermore, they focus on the software engineering phases and are not designed to identify vulnerabilities of already existing systems based on security requirements at the current organisation in which they operate. This is because security requirement frameworks and modelling notations focus on the system-to-be, not the system-as-is. The focus of these approaches is on the modelling and analysis of attacks and vulnerabilities, relating them to security requirements, or capturing and analysing security goals and countermeasures. The organisational context and the current system implementation are not considered - often they are only considered for a specific system. Equally, the operation and change of systems is not taken into account. Therefore, no software engineering approach addresses vulnerability identification of existing systems in an organisational context based on security requirements for the assessment of information security risks.

3.3.3. In business process management

In the workflow and business process modelling field, the principal idea is to integrate or assign risks to business process models to identify risks and evaluate their impact. In this field, the tight relationship between risks and business process models is indeed recognised, as risks endanger the achievement of business objectives. So far, researchers have taken three different directions to align risks and business process models:

1) Create separate models out of the original business process for risk modelling, with regard to aspects like goals, structures and data of the process;
2) Enhance existing business process modelling notations and link risks to process elements;
3) Align risk factors or any other elements used for risk management to business process elements.

All the proposed approaches base themselves on risk management standards, like AS/NZ 4360 (ASNZ, 2004), and use threats and vulnerabilities for all kind of risks - not solely for information security risks. Some of the developed approaches conclude by proposing methods for identifying risks, but propose no method for evaluating and monitoring. Mostly, risks are determined by business values or risk factors and as a subsequent activity, existing business process models are enhanced, duplicated or rebuilt.

The few approaches in the business process modelling and workflow management field that use security requirements are focused on determining the best security solutions based on requirements, rather than on analysis of the current security situation. They define the security requirements for a process or process element, and then determine a security solution. Others integrate security requirements into the business process model. The principal issue of security requirement approaches - such as Herrmann and Herrmann (2006) facilitating security requirements specification and implementation, or Roehrig and Knorr (2004) analysing security requirements and identifying security measures - is that they provide no procedure or method to evaluate, assess or monitor existing security functions (the current state) regarding the adherence to security requirements and

information security risks. These approaches start by considering the business process and determining security requirements for the processes; they then propose the best security controls. Security functions that have already been implemented are neither considered nor evaluated. Furthermore, most of these proposed approaches start from scratch and do not consider the available security functions or re-engineer processes in order to propose the best security solutions to adhere to the security requirements.

3.3.4. Conclusion

In *risk assessments for organisations,* security requirements are used only to determine the impact; in risk assessment in *business process management and software engineering,* security requirements are used for the purpose of creating secure systems or processes. This difference in the usage of security requirements is due to the focus of the approaches in the different fields.

In *business process management,* security requirements are mainly used to determine best solutions for processes or to analyse process security. In this context, security requirements are used as references to determine the best security solution for a process, or are compared with proposals for security design and security mechanisms to design the process securely.

In *software engineering,* frameworks and modelling notations have been developed that support requirement extraction, analysis or visualisation. The objective of these approaches is to produce a set of security requirements that provide “good enough” security against potential attacks. Security requirements are evaluated to discover whether the design or security mechanism of a system to be developed can meet the security requirements.

In *risk assessments for organisations,* security requirements are used for determining the impact of vulnerabilities or to determine whether vulnerabilities are a risk for the organisation. The starting point for risk evaluation is threats and vulnerabilities. Vulnerabilities are determined based on the existence of (identified) threats and the potential violation of security requirements. Only three approaches were identified - NIST SP 800-30 (Stoneburner et al., 2002b), Common Criteria (CC, 2006), and the approach of Innerhofer-Oberperfler and Breu (2006) - that use security requirements as a basis for security evaluation in risk assessments. In NIST SP 800-30, asset-unspecific security standards are used as security requirements; the CC evaluates only the security requirements of a product; and in Innerhofer-Oberperfler and Breu security requirements are used for impact determination but not evaluated.

In current approaches found in the literature in practice and research security requirements and their implementation are not explicitly evaluated to determine vulnerabilities in a risk assessment for an organisation. Therefore with these approaches, one cannot be sure of having identified only true positive vulnerabilities with regard to the business security needs of the organisation.

3.4. Problems of risk assessment

The main three activities of a security risk assessment are risk identification, risk analysis and risk evaluation (ISO, 2009a). Uncertainty is a general problem among these activities. In section 3.4.1 the general limitations regarding risk assessments are presented, categorised into the three key steps of any risk assessment: identification, data collection and assessment. In section 3.4.2, a view on the current practice of risk assessments - in particular, whether security requirements can or are already used and whether vulnerability identification errors do occur are

discussed, based on a survey among security professionals. Section 3.4.3 is about the concrete issues an assessor faces with regard to vulnerability identification and probability estimations.

3.4.1. Procedural limitations

In internationally accepted standards about risk management (e.g. ISO/IEC 31000 (ISO, 2009a)) and specifically in information security risk management (e.g. ISO/IEC 27005:2011 (ISO, 2011c)), the principal steps to determine risks are asset identification, event/threat identification, vulnerability/control identification, likelihood determination and impact analysis. Within the literature, many limitations of risk assessment approaches are provided. All this critique can be categorised into three activities of any risk assessment: identification, data collection and assessment.

(1) The identification category is about activities undertaken to determine, for example, an event. A threat that uses vulnerabilities is defined as an event (ISO, 2011c). The identification of threats and vulnerabilities is challenging, as underlying conditions change constantly, through development of new technologies, new competitors, new laws, etc. (Jackson, 2007). Therefore, threats and vulnerabilities are not static; their behaviour and seriousness can change rapidly, often within days. Threats and vulnerabilities are identified based on security expert knowledge, usage of security scanning tools and publicly available data. Security experts use implicit knowledge and experience, as well as explicit data such as vulnerability lists, for risk identification. But how does one know and how can one verify whether or not all threats and vulnerabilities have been identified correctly and completely? Furthermore, events within associated

companies (e.g. outsourcing partners or inter-company process chain partners) cannot necessarily be discovered; they are beyond company boundaries. However, these events could potentially negatively affect a company, as business processes and systems are heavily interconnected nowadays (Kinney, 2003).

(2) The data category is about the data needed for the evaluation of risks. For the impact and probability assessment of a risk, data regarding the impact and probability of an event in a given situation is needed. The major issues here are that exhaustive public data of events, impacts and their respective probabilities are not available (Stewart, 2004), and internal historic data are not available for the estimation of the impact of possible changes on the company. For example, the event may not have occurred in this type of industry yet, within the company or within the scope of the particular situation. If no comparable data is available, best guesses must be used for determining the change's impact and probability. But how to make such a best guess in an environment where one knows little about the population, to determine the occurrence rates, effects or impact of the events? In case the event data is available, internal data about events in companies can still be incomplete, or may represent a "lucky" history (Frachot and Roncalli, 2002) and thus quickly become obsolete. In addition, internal historic event data may not represent a true view, and the number of events recorded could be lower than the true number (Frachot and Roncalli, 2002). For example, the claims data recorded regarding the occurrence rate and extent of loss, are often below the average of the reference industry or of competitors. Another issue is that probability distributions become incorrect as they are based on historic data, not representing modern event behaviour changes (Stiglitz, 2008). For example, 100-year events

reoccur nowadays every 10 years in fat-tailed distributions. How can one verify that the data used for the assessment are still correct?

(3) The assessment category is about activities or models to evaluate the change's impact. Risk assessment is based on the impact and the probability of the event. The models used to determine risks and dependencies are poor, because co-occurrence of risks, uncertainty between event relationships and different assessment scales are not considered. Co-occurrence of events leads to indeterminable impacts and damages, because the events might occur in associated companies; that, in turn, may have an impact on other risks that are not considered when they are evaluated in isolation. In the current methods, the assessments are performed on decomposed model elements but do not consider the organisation as a whole. Furthermore, there is uncertainty between the relationship of an event and its impact. For example, where the impact of the event is not known, or is dependent on other conditions/parameters. However, side effects (multiple impacts or dependencies) or parameters are not considered, and uncertainty is assessed by gut feeling, or by subjective security expert knowledge (Stewart, 2004). Although safeguards put in place are considered in the impact assessment, they are evaluated for a particular threat/vulnerability, and the side effects of other events are not considered. How does one determine that safeguards are implemented and operated as intended? A systematic assessment of the safeguards regarding secure operation, secure design and effectiveness is currently missing. Furthermore, probabilities are measured by different techniques - by both quantitative and qualitative methods. But the comparability of qualitative and quantitative assessments of risks or probabilities within an assessment method is not validated. Furthermore, assessments are influenced by perceptions

(Stewart, 2004). Behavioural biases as a result of the educational background, organisational level or positive/negative attitude of the assessor may also affect the assessment of events, probabilities of occurrence or the impact estimation - assessments always involve subjective judgement (Redmill, 2002). In addition, current risk assessment procedures lead to simplification, and are focused too strongly on technical issues rather than on information or business issues (Gerber et al., 2001). For procedural reasons, the assessor will usually simplify, otherwise he will be lost in detail and forget the objectives (Halliday et al., 1996). Additionally, methods follow the waterfall model and therefore are not capable of considering changes during the lifetime of the assessment (Vidalis, 2004).

The limitations of information security risk assessments are related to uncertainty about the occurrence of threats and vulnerabilities (Kinney, 2003), as well as future or unknown events (Pieters and Consoli, 2009). Questions which arise include: how likely are events? What is the impact of events? Can one anticipate risk? Basically, for the risk assessment, one does not have reliable and accurate data on events' probabilities and their impact on the company (Stewart, 2004). Another problem is the complexity of the real world, considering all its variables, where models are likely to fail. Risk assessments are mainly based on estimations, assumptions, simplifications and causal dependencies (McKenna, 2001), and the objectivity of risk and security are often implicitly assumed (Pieters and Consoli, 2009). An additional aspect is risk perception influencing people's behaviour (Sjöberg et al., 2004) - that's to say, the subjective assessment of an event and its (negative) impact. Risk perception is not only about individuals. It also has a social and cultural component, reflected in values, symbols or the history of a group of people. Risk perception is not discussed in detail in this thesis, but subjectivity

caused by perception is also a problem of risk assessment results. However, no matter how objective or subjective risk assessments are, they are necessary to determine risks and to apply the appropriate security functions. But an attempt should be made to identify vulnerabilities and risks accurately to reflect the current risk situation for an organisation.

3.4.2. A survey among practitioner's

In a lecture at an information security conference on February 25th 2011 the 55 participants, all security professionals, were interviewed in the form of a questionnaire and a quasi-experiment regarding IS risk assessments and the application of security requirements. The objective of the survey was to examine the current practice of risk assessments - in particular, the procedures and concepts used in risk assessments, the trust in risk assessment results, the evaluation of security controls and the usage of security requirements, as well as the availability of process models. One further aspect examined was whether security requirements and business process models positively support the identification of vulnerabilities and risks. The survey consisted of three parts; parts 1 and 2 were made up of a questionnaire with multiple-choice questions where participants were able to tick multiple answers and able to add own answers. Part 3 formed a quasi-experiment, where participants had to perform a risk assessment task and to document their risks identified. The questionnaire was verified in a test run beforehand, to ascertain to what extent the questions are understood and the responses can be evaluated. The design of the quasi-experiment (part 3) was also tested, in a trial, by an individual with the same background as the conference participants with regard to understandability, time required and the results

generated. In the following, a description of the content and aims of parts 1, 2 and 3 is provided:

Part 1 contained questions about IT risk assessment, in particular, about what criteria are used and how risk results are valued. This part of the survey mainly dealt with what methods are used, the purpose of risk assessments and what - and to what extent - concepts are used by practitioners. The questions were based on the security risk assessment concepts, methods and procedures identified in the literature review. The aim of these questions was to determine the current practice regarding risk assessments in the industry, as well as how familiar practitioners are with security risk concepts.

Part 2 concerned the use of business process models, classification of data in enterprises and the use of security requirements in risk assessments. Here, the questions were about the availability of business process models, as well as about risk identification with security requirements. The questions were based on the hypothesis that security requirements and business process models can be (re)used for vulnerability identification and could resolve identification errors. Basically, the aim was to get to know whether process models and security requirements are available, whether risks identified by security requirements are perceived as being more accurate, whether security requirements are used, and to what extent they are used in assessments.

Part 3 contained a risk assessment task. The survey's participants had to carry out a risk assessment based on different sets of information given. The example used for this task was a real world business process model, a risk analysis describing the business case and risks identified, and a security requirements description relevant to the business case. Participants had to identify and

document on a blank page the vulnerabilities/risks, and determine their probability and impact. The objective was to verify whether vulnerabilities are identified more accurately by participants if information such as security requirements or a business process model is available. This part of the survey was used for validation; to determine that security requirements and business process models can help to resolve vulnerability identification errors (see section 6.4 for details), as a higher accuracy and precision might be achieved.

The survey took place in a closed room under supervision. The participants had approximately 30 minutes' time to answer the questionnaire. Out of all 55 participants, 45 answered part 1 and 46 answered part 2. Part 3 of the questionnaire was performed by 36 participants. Multiple answers were allowed for some questions. In the following, a brief overview of the results is presented. The detailed survey results can be found in the appendix.

Survey results - Parts 1 and 2

The aim of the survey was to investigate the following hypotheses at part 1 and 2 from the perspective of security specialists in the field, and to what extent these hypotheses can be confirmed or denied based on the answers of the questionnaire. The hypotheses were drafted as a result of the literature review in order to determine whether security requirements and business process models can be - or are already - used for vulnerability identification.

Hypothesis 1: Risk assessment procedures are considered as inadequate by security experts due to the subjectivity of results, insufficient data for assessments, the accumulation of risk and inadequate consideration of frequencies.

Risk assessment procedures are considered in practice as procedures with shortcomings, but not completely rejected because of their deficiencies. It was confirmed that risks cannot be determined objectively and vulnerability identification errors do occur because of insufficient data. However, risk assessments are not considered to be subjective by the participants, even when they are influenced by external events. The accumulation of risk results, e.g. of medium or high risk, was not identified as a problem or recognised as such in practice. Furthermore, the frequency of events is often not considered in risk assessments as reported. Participants specified that assessment procedures should improve, particularly in the integration and combination of compliance and risk management, and in the efficiency of the assessment process. The existing assessment procedures are largely considered to be adequate by the participants.

Hypothesis 2: All security controls are reviewed in risk assessments as proposed by best practice standards.

The survey reflects a mixed picture. Security controls are partially not evaluated, or possibly only for assets with weaknesses. Another group of the participants evaluates security controls for assets which are assessed in the context of risk assessment. However, a systematic assessment of security controls for all assets is not conducted.

Hypothesis 3: Business process models are available and up-to-date in practice.

The survey has confirmed that business process models for critical and important processes at companies are both available and up-to-date. Mainly actors, activities and IT systems are represented in the business process models. Risks, security controls and security requirements are not modelled. As drivers for business

process modelling, efficiency gains and cost reduction (as well as regulatory requirements) are seen by the participants.

Hypothesis 4: Security requirements are in part considered in the risk assessment, but not systematically used for the assessment of risks.

Security requirements are defined for IT systems and data, and are usually described in the relevant security policies/guidelines. Security requirements are usually considered in risk assessments. To what extent security requirements are systematically used in risk assessments (especially for vulnerability identification) could not be verified in the survey. However, due to the fact that best practice methods are used based on threats/vulnerabilities, and that survey participants had often not mentioned security controls and security requirements as criteria in risk assessments in part 1 of the survey, it is assumed that security requirements are not systematically used for vulnerability identification.

Hypothesis 5: Security requirements are used in risk assessments; they are defined for assets and used to measure risks.

Security requirements are used in the risk assessment for assets (IT systems and data) as well as for assets defined. There is no active measurement of risk, but security requirements are used to verify data security.

Hypothesis 6: Data is classified throughout the company.

At 90 percent of the participants' companies, IT systems and/or data are classified according to confidentiality, integrity and availability. Data classification is considered in the description of security requirements and, as such, the classification is available in risk assessments.

To conclude, the participants of the survey consider a risk assessment as a procedure with shortcomings, but do not completely reject the concept. Participants report that risks cannot be determined objectively and vulnerability identification errors occur. Mostly, security best practices and checklists are used. Security functions are not completely evaluated for all assets in assessments and security requirements are partly used - but not systematically to identify vulnerabilities.

3.4.3. Determing probabilities - An example

In general in a security risk assessment, after having identified the assets, the assessor begins by determining threats that could occur, and then cites any existing vulnerability. For the identification of threats and vulnerabilities, the assessor uses security best practices, a list of threats and vulnerabilities or security controls, and his own experiences. Different sources of information are used to identify threats and vulnerabilities. The problems start with the fact that one cannot determine whether the threat, vulnerability or security control lists used are complete and comprehensive. These lists are compiled by governmental or business organisations, without making a claim of being complete; they are updated sporadically. In addition, these security control practices - as well as threat and vulnerability lists - are based on past experience. This may not present a true view; as a result, these sources do not contain all threats or vulnerabilities which could occur and thus have a negative impact. Threats/vulnerabilities that have not occurred yet or were deemed as negligible - as well as specific security controls - are not necessarily seen as best practice. It is not only that these lists may not contain negligible threats, but also that the assessor tends to omit

irrelevant or very unlikely threats like earthquakes or espionage, as these do not happen very often, *based on his experience*. Furthermore, to determine the likelihood and impact of threats and vulnerabilities, there is no detailed guidance available - only general advice. Risk assessment approaches like, for example, NIST SP 800-30 (Stoneburner et al., 2002b) do not describe how to link threat sources with vulnerabilities, or how to derive and rate any probabilities. Further questions arise: Does the probability estimation represent a true view? How does one validate the estimations? If you use qualitative or quantitative thresholds for ratings, these limits have to be reasonable in the context of all vulnerabilities and risks identified, in order to compare them among each other. These limits are likely to be too high or low for some of the risks identified, as they have to be suitable across the organisation. In addition, the aggregation of probability values causes problems; it might pervert the probability to a minimum and the effects to systems (and whether they are single or multiple effects) cannot be reliably estimated. If the maximum value is used, this may be an overrepresentation and an average may be an underestimation. It is also dependent on the number of estimates. A joint probability calculation of independent events leads to a decreased value, as the lowest value determines the probability. Furthermore, the consequences and the existence of misestimating are not considered. Misestimating, as well as the existence of ambiguity and the aggregation of risk, creates a measurement risk not indicated in the assessments. Another issue is psychological phenomena; the assessor can be influenced by emotional factors. These can be based on experience or social groups, negative media on technology or commercials, as well as concentrating on severity (Stewart, 2004).

There is a lot of uncertainty in the estimation of probabilities to determine which might be a ‘real’ risk for a company. In order to showcase the issues of estimating probabilities in an uncertain environment, a probability calculation of a hypothetical encryption vulnerability at a web server is conducted. In the following, the probabilities of the following outcomes for the web server will be outlined:

- A criminal exploits the encryption weakness in the webserver;
- A hacker exploits the encryption weakness in the webserver;
- A hacker or a criminal exploits the encryption weakness in the webserver;
- The likeliness that a hacker or criminal is not able to exploit any weakness.

To determine the probabilities of the identified web server threats, further data is needed and parameters that are associated with this scenario must be considered. The following data were identified to be considered for the probability evaluation and evaluated as to whether they were available:

- The number of known exploits for the webserver version: the number of exploits should be determinable by publicly reported bugs/vulnerabilities;
- The number of unsecured exploits for the webserver version: the number of unsecured exploits should be determinable by a security analysis;
- The criticality of exploits: this is determinable, as exploits are rated by security organisations;
- The detection rate of all vulnerabilities by a malicious user: this ratio is not determinable as the ratio is dependent on the knowledge, available tools and number of exploits/vulnerabilities available;
- The ratio of successful exploiting: this is also indeterminable - it is dependent on the knowledge of the malicious users, the complexity of

vulnerability as well as the motive, resources and available time of the malicious user;

- The number of users of the web server application: this can be determined by page views and IP-address matching;
- The relation of friendly and malicious users accessing the webserver: again, not determinable and dependent on popularity of the company, fame for successful breach, monetary gain, etc.;
- The impact of controls: this is not considered explicitly, as a firewall prevents an attack. Implicitly, controls are considered in the ratio of successful exploiting;

Out of the data that was considered as necessary to determine the probabilities, a tree diagram was created to show the dependency between the parameters (see Figure 3-9). Furthermore, this is useful for the probability estimation.

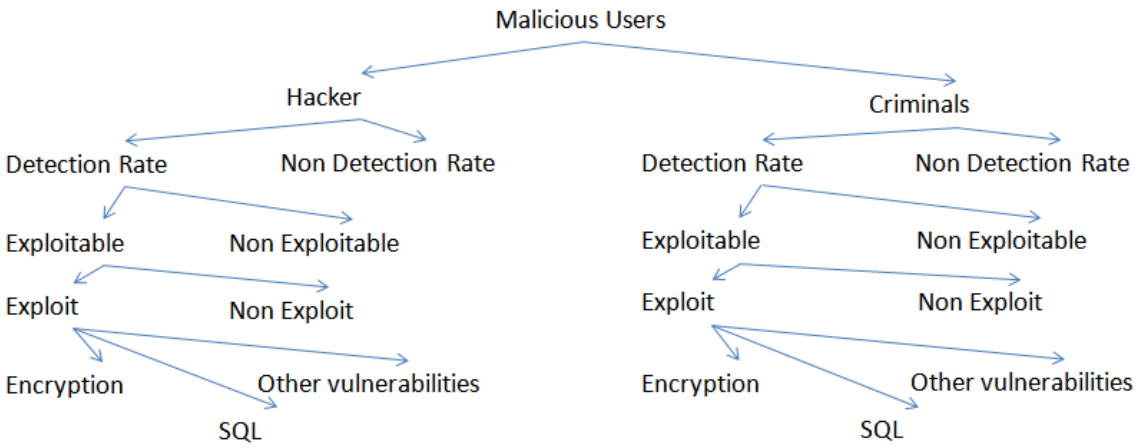


Figure 3-9 Dependency tree

The malicious users accessing the website are separated into two groups - hackers and criminals - as identified in the threat analysis previously. The sub-levels below hackers and criminals are the same. Each has been assigned a

detection ratio for vulnerabilities - i.e., the probability that they are successful detecting the vulnerabilities. Next follows the ratio of exploitable vulnerabilities; only a few vulnerabilities are exploitable as they were not secured. The next level is about whether the hacker/criminal is capable of exploiting unsecured vulnerabilities. The last level of the tree is the probability that this vulnerability is exploited; some are likely to be more exploited than others. In this example, the independency of variables (e.g. hacker, criminal, the encryption and SQL vulnerability) is assumed. However, it is often hard to determine whether parameters are independent, because knowledge is necessary about intentions (e.g. that's the difference between a hacker and criminal), technical details of vulnerabilities (e.g. details about the encryption and SQL issue) and the environment (e.g. applied administrative and technical security functions) of the parameters and their relationship to each other.

The following figure shows the assigned probability values of the security expert for each parameter of the tree. Most of the probability values in the dependency tree are only an expert judgement, with no claim of being valid. Rather, these artificial values are used to showcase how the overall probability is affected by single values, as well as being able to provide a probability statement about the hacker and criminal exploiting the webserver to help answer the questions posed at the beginning.

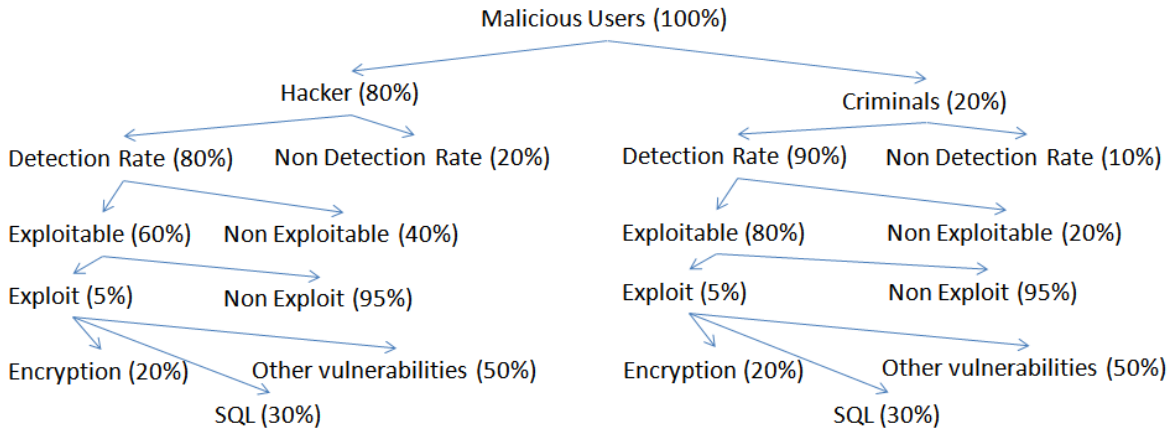


Figure 3-10 Dependency tree with probabilities

Before presenting the detailed probability estimation results for the hacker and criminal, one would expect that the webserver is a medium risk. The results for the probabilities from the start of this analysis are as follows:

- A criminal exploits the encryption weakness in the web server = 0.144 percent of malicious users (nobody);
- A hacker exploits the encryption weakness in the web server = 0.384 percent of malicious users (nobody);
- A hacker or a criminal exploits the encryption weakness in the web server = 0.528 percent (nobody);
- The likeliness that a hacker or criminal does not exploit any weakness = 97.36 percent.

One can notice that there is a discrepancy between the expectation of the risk (rated as medium) and the detailed calculation (not very likely). Even if you change the obviously small exploitable ratio (Exploit (5%) and Non exploit (95%) in the tree) for the hacker and criminal from 5 percent to 50 percent, the results change for the hacker by 3.5 percent, for the criminal by 1.3 percent and the combined

result by 4.7 percent. The likeliness that both do not exploit any weakness decreases by (only) 24 percent. Based on the results and the experiences when changing some ratios, the following can be noted:

Dependencies: There is a direct dependency of the result to single parameters, i.e., a reduction/increase of one parameter leads to a reduction/increase of the result by the same percentage. Therefore the percentage of misestimating is relevant, not the absolute amount. For example, if the single value of the exploitable ratio changes from 5 to 10 percent (100 percent increase) then the results change in the same ratio (100 percent). Especially changes of low probability values have a huge impact on the overall result.

Baseline: The base of the probability has to be specified. A probability of, say, 12 percent has no significance without knowing the total population. This is especially true when populations are further linked - like the malicious-to-normal users ratio.

Probability: The total probability (the result) tends towards 0 or 100 percent in a chain of parameters, as the total probability is below/above the smallest/largest single value and small/large values are always existent. Therefore the significance of the result is disputable; it may be perceived as negligible because of the total probability value. Furthermore, results are blurred by the use of estimates; there is also no knowledge whether the base for the estimates follows any probability distribution, and one does not know the standard deviation.

Tree diagram: Determination of the dependencies of the different factors is partly difficult as dependencies are not precisely known. This makes the construction of a correct tree diagram difficult, which, in turn, has an impact on the probability question “what would you like to know?” as the tree diagram is used for answering this question.

Perception: The perception of the results is dependent on the probability statement and the size of the result value. For example, do you class the likelihood of an event as 95 percent unlikely or 5 percent likely? A higher percentage is assumed to provide more confidence (perception), and the perceived significance of the result can be higher if negative probability statements are used, e.g. likeliness that a malicious user does not exploit a weakness.

Even if the probability ratios in the example might be incorrect, the example shows that vulnerability identification and probability estimation are both processes of high uncertainty. To identify and to determine events, probabilities and impacts correctly we must have comprehensive knowledge about the environment of the risk, the company and outside world. This would require that associated parameters, corresponding probabilities, the basic population, and correlations are known, immediately updated, based on enough statistical data and can be modelled. But this data is often not available, may be compromised, cannot be reliably verified and modelled; the real world is too complex and unpredictable. From that perspective, using probabilities in a risk assessment in an uncertain environment where these data are not available leads to over- or under-representation of the risks of an organisation.

3.5. Research questions

Different risk assessment methods have been developed in business and governmental areas. They have been applied to specific problems but using the same concepts, which are described in information security standards. Events, threats and vulnerabilities are the starting points, along with security requirements, of any risk assessment method. In *business process management*, as well as in

software engineering, security requirements are analysed to ensure the secure design and security functions of a system to be developed, but not to verify implemented security functions (the current state) and to identify vulnerabilities. These approaches are helpful to define the best security functions for systems, but are not suitable for determining the organisation's information security risk. However, *in business process management* and *software engineering*, security requirements provide the starting-point for any analysis of the security system design and security function implementation; and therefore they could help to determine vulnerabilities more accurately and provide a measurement criterion for security. In *risk assessments for organisations*, security requirements are used to determine the impact of vulnerabilities and the presence of vulnerabilities or security functions. However, security requirements of (information) assets are not explicitly analysed to identify vulnerabilities with regard to the security design or security functions. Usually, brainstorming, security testing, security and vulnerability checklists as well as best practices are used to determine events and the vulnerabilities of single assets. But these data are uncertain – they are asset-unspecific - and they do not consider (inter-)organisational differences and their security requirements (Siponen and Willison, 2009) seriously enough. There is a risk that inefficient security solutions are applied, substantial threats are ignored (false negatives) and companies may believe in inaccurate results (Fenz and Ekelhart, 2011). This uncertainty in the assessment procedure was also shown in section 3.4 through the discussion on procedural limitations of approaches, the probability estimation example and the survey among security professionals. Furthermore, with the methods used in current approaches like security testing, only the presence of vulnerabilities can be proved - not their absence (Wang, 2005) - as only security issues are identified. The true value - the security needed,

represented by security requirements - is not evaluated. One cause for the lack of consideration of security requirements in risk identification lies in the definition of risk - based on threats, vulnerabilities and impact. Another reason is that security requirements tend to come after identifying vulnerabilities. This means that security requirements are drafted after identifying risks, and after the decision on risk treatment has been taken. However, this neglects the fact that risk assessments are recurring activities and security requirements are usually already available and drafted for assets, for example, in security policies and procedures as reported by the survey participants of section 3.4.2.

Because vulnerability identification errors (false positives and negatives) can cause a company to invest in security functions that are not required and that are not compliant to any governmental regulations, or can lead to unwanted losses, resolving vulnerability identification errors would help to reduce the security risks of a company. Therefore, the research objective of this work is to utilise security requirements and business context-dependent information at the vulnerability identification phase of security risk assessments for the purpose of resolving vulnerability identification errors (false positives) and help to resolve false negatives. The following research questions have been formulated to achieve the research objective as defined in section 1.3. The results of this work enhance the understanding of security requirements within information security risk assessments for vulnerability identification. Question 1 was already answered with the discussion of the current state of the literature in section 3.3 and the discussion of the problems of risk assessment in section 3.4.

1) Are security requirements already used for vulnerability identification in risk assessments in current approaches? Do vulnerability identification errors occur and are they reported by security practitioners?

The discussion of the literature (see section 3.3) shows that, in current security risk assessment approaches, security requirements are used to determine the impact of vulnerabilities, but not for their identification. Asset-specific security requirements are not evaluated to identify any vulnerability. Furthermore, from the discussion of the limitations of risk assessment approaches (section 3.4.1), it can be concluded that vulnerability errors occur because of uncertainties about current and future events and threats. In addition, the probability assessment example (see section 3.4.3) shows that there is uncertainty in determining probabilities; this also causes errors in vulnerability occurrence rates. Survey participants (see section 3.4.2) also report that risk assessment results are subjective and vulnerability identification errors can occur; assessments are valued as error-prone.

2) How are vulnerabilities, risks, security requirements and security controls related and can risks be determined by evaluating security requirements, as a risk is defined by vulnerabilities and impact? How should risk be defined in order to use security requirements for identifying risks and vulnerabilities through their evaluation in business process models?

   Concepts of security risk management and assessment, and their relationships to each other, are described by information security models as shown in section 1.2. These models define the elements, terminology and their relationships, as well as forming the basis for security risk assessment and management. One contribution of this thesis is an extended information security model showing the relation between risk-, asset- and security-related concepts (see section 4.1). It also provides a security requirements definition of risk. The extended information security model provides the foundation for determining vulnerabilities and risks by

security requirements in information security risk assessments - besides using events, probabilities and impact for risk identification. The model also helps to understand the relations between risk-, asset- and security-related concepts.

3) Can a security requirements and business process model based approach help to resolve vulnerability identification errors (false positives and false negatives)? Does the accuracy of identified vulnerabilities increase (true positives), and vulnerability identification errors decrease (false positives), by explicitly evaluating security requirements by means of business process models?

   With the proposed security requirements risk assessment approach called 'SRA' (chapter 5) and validation work (chapter 6), evidence is provided that vulnerability identification errors can be resolved by explicitly evaluating security requirements in the business process context. Within the validation, a best practice security risk assessment approach and the proposed approach are both applied to several real-world examples within an insurance company, and the results' accuracy compared. In addition, the quasi-experiment results of the survey are used for validation, to show that vulnerability identification errors can be reduced by using security requirements and business process models.

3.6. Research methodology

The validation and verification of results is a well-recognised activity in the scientific community to test hypotheses. Verification surrounds the truth or accuracy of the theory, methods or model developed, whilst validity is about

relevance and significance. In applied research, experiments are used to validate and test hypotheses. According to Wallace and Zelkowitz (1997), experimentation in computer science can be grouped into one of three methods:

- Observational methods collect data on an ongoing activity (e.g. project monitoring, case study, assertion and field study);
- Historical methods collect data on already finished activities (e.g. literature searches, legacy data, lessons-learned and static analysis);
- Controlled methods are about collection of statistical data to prove validity (e.g. replicated experiments, synthetic environment experiments, dynamic analysis and simulation).

An overview and explanation of research methods in computer science can be found in Holz et al. (2006), and in computer science, observational methods like lessons learned, assertion and case studies are most often used (Wallace and Zelkowitz, 1997). Therefore, in the following paragraphs, observational methods are discussed and considered for the verification and validation of the security requirements risk assessment approach in this thesis. To validate work in computer science the following methods are most often used:

1) Case study;
2) Constructed examples;
3) Testing on real examples;
4) Controlled experiment.

1) Case study

This method for verification and validation would be based on an existing case study containing business process models. The proposed approach would be applied to the case study and the results of the two would then be compared. Such

a case study must provide details about the business processes, systems, underlying conditions (technical, economic and behavioural), the risk assessment results and procedure of the applied risk assessment approaches to be reused.

After an extensive search of both the published literature and publicly available information, a case study complying with these requirements was not found. Case studies or papers about current practices on business process models are rarely available (zur Muehlen, 2007), because research mostly focuses on enhancing of business process models and their effects, e.g. modelling languages (zur Muehlen, 2007) or project outcomes (Eikebrokk et al., 2008). There are some other business process management case studies to which process models were applied, as for instance in organisational change (Mendes et al., 2003) or in healthcare (Becker et al., 2007). But these studies do not provide models or enough details to use them for validation and verification.

2) Constructed examples

This method for verification and validation would use a constructed example of a problem. The proposed approach would be applied to that example and the results then interpreted. This method has the advantage that:

- the examples can be illustrative regarding the contribution;
- examples can be changed to lead to alternative results;
- the approach and results can be properly depicted.

However, constructed examples have the disadvantage that they may mask problems which would have occurred in the real world, or that they may merely reflect the theory. In addition, these examples may be too focused on one specific

problem; key parameters that influence the results may be accidentally or deliberately omitted.

Constructed examples are used in the problem domain, for example, by Innerhofer–Oberperfler and Breu (2006) to discuss and showcase the developed approach. Matulevicius et al. (2008) also use a real world running example to demonstrate the applicability of their approach. But the examples used by them could not be used for validation, as details are missing or are too specific to the applied problem. In this thesis, constructed examples are used only for the presentation of the security requirements risk assessment approach (as in section 5.3) because of the disadvantages mentioned previously.

3) Testing

This method for verification and validation would use an example taken from the real world. The proposed approach would be applied to the real world example and the results then compared to the results of an applied alternative approach. This requires that the work should be conducted twice and the underlying conditions be the same for both approaches. To use this method successfully, some conditions also have to be met:

- The assessed real world example should be complex, but not too complex and not too large;
- two different teams have to apply one of the approaches with people with the same skills and information on the environment;
- the assessments have to be conducted in the same time period to guarantee having equal underlying conditions.

Testing is often used by researchers to verify their developed methods. For example, Mayer (2009) and Haley (2007) both validate their model- and security-requirements-based approaches by testing at companies. However, the validation cases used cannot for the most part be reused, as the test environment has technically, organisationally or socially changed and cannot be re-established. This is also because the specifics are not described in every detail. The security requirements risk assessment approach in this thesis will also be validated and verified by testing at a global insurance company. The proposed approach and an existing alternative approach are applied to the same real world examples, and the results and differences compared regarding their accuracy. The difference in this thesis - compared to other works - is that two different approaches are applied three times and results compared, while others only apply their approach to the real world once and interpret their results from that.

4) Controlled experiment

This method for validation would use reference groups where the results from one experimental sample are compared against the control sample. The difference between the two groups (the control and experiment group) would be the only effect to be tested. The two groups should be probabilistically equal, which means that the groups should act in the same manner with the information provided, and the measurement of the effects should be performed in the same way. With a controlled experiment, the security requirement risk assessment approach and a best practice risk assessment approach would be performed by two groups and the results compared against each other. But this would require that the group applying the security requirement assessment approach has enough knowledge of the approach, the risk situation is described without interpretation, and assessors

have similar risk knowledge, which might not be achievable in practice. Such an experiment would have too many variables (e.g. individuals' knowledge about security risk assessments, or about threats and vulnerabilities, or the learning curve of the approaches) on which the result is dependent. Therefore, to apply two different approaches in an experimental setting - and to compare results and determine the effects - would not lead to meaningful results.

In published computer science and software engineering articles, experiments are used only in about 2-3% of works, as reported by Wallace and Zelkowitz (1997) and Sjoeberg et al. (2005) for the years 1985, 1990, 1995 and in the decade from 1993 to 2002. None of the work related to the proposed approach identified in the literature review uses experiments to verify their proposed procedures. These could therefore not be used as reference points. In this thesis, a quasi-experiment is performed to demonstrate that vulnerability identification errors can be resolved by providing additional sets of information on the same risk description (the grouping variable). In the quasi-experiment, individuals were not randomly assigned (which would be the case in an experiment), but rather the experiment was embedded in a survey at an information security conference. However, the participants were randomly provided with different sets of information (all participants got a risk description, two-thirds also got a business process model, and one-third a security requirements description) to identify risks and vulnerabilities. The effect to be tested was whether predefined risks included in the risk description were identified with different accuracy by the additional information provided, and whether vulnerability identification errors occurred (the dependent variable). The design of the quasi-experiment had been tested previously in a trial run by an individual with the same background as the information security

conference participants, to assess its comprehensibility, time required and the results generated by the different sets of information.

3.7. Chapter summary

Risk assessments are conducted in various fields, and focus on different aspects of different areas. Therefore, different risk assessment methods were developed in both business and governmental areas, applying to specific problems but building on the concepts of threat and vulnerabilities defining a risk. These concepts and the associated terminology are described in information security standards and form the basis of any risk assessment method. Events, threats and vulnerabilities are the starting point to determine risks, along with security requirements. Current information security risk assessment approaches for organisations use only security requirements to determine the impact and consequence of a vulnerability: however, they are not explicitly evaluated to identify them. Furthermore, current risk assessments have limitations in identifying vulnerabilities as well as in estimating probabilities accurately - all are related to uncertainty, causing false negatives and positives. Security requirements could help to determine vulnerabilities more accurately, as they specify the necessary security *and* provide a measurement criterion. Therefore, the research objective of this work is to utilise security requirements and business context-dependent information at the vulnerability identification phase of security risk assessments for the purpose of resolving vulnerability identification errors (false negatives). This would help to reduce security risks for a company; thereby, they could invest more efficiently in security. A security requirements risk assessment approach called ‘SRA’ will be developed, to resolve vulnerability identification errors. It will be validated by testing and a quasi-experiment.

Chapter 4 - Security Requirements based Risk Assessment

In this chapter, the fundamental concepts for security requirements risk assessment approach called ‘SRA’ are illustrated. In order to understand why and how security requirements and business process models can help to resolve vulnerability identification errors, the underlying concepts are presented in general, before details of the SRA are given in chapter 5. Therefore, this chapter first explains the fundamental principles of concepts, the rationale as to why these concepts can be used, as well as how they are used in a security requirement risk assessment approach. An extended information security model describing the relationships between risk and vulnerability, and between security requirements and assets, is presented. The connection between risk, vulnerability and security requirements is re-defined, thereby allowing a risk definition based on security requirements. Using this definition of risk as well as business process model information, it is then illustrated how security requirements and business process models can be used in evaluating risks and vulnerabilities. Because security requirements represent security needs, define the desired security and can be used as a measurement value for security, they allow more accurate identification of vulnerabilities; they can provide a more informed statement about the security of an organisation. Furthermore, the elicitation of security requirements is discussed and a structure for security requirements’ characterisation is defined, based on business process model information supporting the assessment process. This chapter concludes with a discussion of why and how security requirements’

interdependencies on information assets between business processes can be considered, before the proposed approach is explained in detail in the next chapter.

4.1. An extended information security model

Information security models were compiled to present the fundamental concepts and their relationships in security risk management and assessment. The conceptual relations - e.g. between assets, threats, vulnerabilities, impact and security requirements - are demonstrated by means of information security models by other researchers such as Stølen et al. (2002), Matulevicius et al. (2008) and Innerhofer–Oberperfler and Breu (2006) as described in chapter 1. To reiterate, these models provide a basis for a common understanding about the relationships between the different elements used in security risk management. A relationship connects elements of the model and describes their links to others. An element represents a concept (e.g. risk) or part of the concept (e.g. vulnerabilities, threats and events defining a risk).

The IS models of chapter 1 define risk based on threats and vulnerabilities. In this thesis risk is defined by security requirements. But before defining risk based on security requirements, the models presented in chapter 1 are compared to see whether relations between risk and security requirements are already defined. Before the comparison, core definitions of the elements are provided which will be used later in this section for the extended information security model, which is based on these three models using similar terminology. The core definitions of the elements are as follows:

A security objective is a high level description of the security to be achieved; security is the protection of information. The security objective is driven by business requirements that are affected by risks. Business requirements describe security needs from a business operations perspective, where the business operation is a set of activities that is defined and can be modelled as a business process. A security requirement is a refinement and further specification of the security objective, and represents constraints on the functions of the system, where these constraints operationalize one or more security objectives (Haley et al., 2008). Risk treatment is the process of selection and implementation of security functions to modify risk based on security requirements. A security function implements security requirements in the form of administrative, physical or technical controls and is applied to an asset to adhere to the security requirement. Assurance is about the evaluation of a security function, and is used to establish whether the security requirements are adhered to. Assurance gives confidence that security functions reduce risks to assets and assets are protected according to the requirements. An asset can consist of hardware, software, information systems or any physical assets used to fulfil the business requirements of an organisation. An information asset is a refinement of an asset consisting of data. A risk is the combination of a probable event and its impact, which would result in the violation of security objectives. An impact is an adverse change of an event that violates the security objectives on an asset. An event is a threat that exploits a form of vulnerability. A vulnerability is a weakness of an asset or control related to the security objective, and a threat is a potential attack or incident that could lead to a negative impact on an asset.

Table 4-1 compares the elements used in the models of Stølen et al., Matulevicius et al. and Innerhofer-Oberperfler and Breu against the elements used in the

extended information security model. This comparison shows that the models are built on the same core concepts. But elements like assurance and business requirements are missing in the models, linking security risk assessment with the business process management field.

Table 4-1: Comparison of model elements and concepts of risk

Model elements	Innerhofer–Oberperfler and Breu (2006)	Matulevicius et al. (2008)	Stølen et al. (2002)
Threat	Threat	Threat	Threat
Vulnerability	Agent	Vulnerability	Vulnerability
Event	Incident	Event	Not used
Impact	Threat	Impact	Likelihood and Consequence
Risk	Threat	Risk	Risk
Risk treatment	Security solution	Risk treatment	Not used
Element/Asset	Model element	Asset	Asset
Security function	Security Control	Control	Security Policy
Security Requirement	Security Requirement	Security Requirement	Security Requirement
Security objective	Business Security Objective	Security criterion	Target of evaluation
Assurance	Not used	Not used	Not used
Business requirements	Not used	Not used	Not used
Business process modelling	Not used	Not used	Not used

The three models - of Stølen et al. (2002), Matulevicius et al. (2008) and Innerhofer–Oberperfler and Breu (2006) - are based on the definition of risk being threats and vulnerabilities; they do not consider security requirements for determining a risk. Therefore, these models are missing the relationships between risk, controls, security requirements and assets. Furthermore different terminology is used for some of the concepts used.

Table 4-2 identifies which links between risk/ vulnerabilities and security objectives/ requirements are present and which are not in these models. For example, Stølen et al. (2002) did not consider controls as an element; nor did they

consider security requirements that were not directly linked to risks or assets. Matulevicius et al. (2008) made no link between the security requirement and control to an asset. Innerhofer–Oberperfler and Breu (2006) did not consider risk as an element, apart from noting that there is no direct link between security controls, security requirements and assets.

Table 4-2: Comparison of security requirements usage

Relations	**Innerhofer–Oberperfler and Breu (2006)**	**Matulevicius *et al.* (2008)**	**Stølen *et al.* (2002)**
Risk to security objective	No	Yes	No
Risk to security requirement	No	Yes	No
Risk to business requirements	No	No	No
Vulnerability to security objective	No	No	No
Vulnerability to security requirement	Yes	No	No

As none of these models address relations between risk, security requirements, security controls and assets, an extended information-security model (see Figure 4-1) is introduced to build on the previous models and represent these relations. This extended information security model supports the consideration of risk from a security requirements perspective, as it provides a combined view on concepts related to risk, risk treatment and security requirements.

This extended information-security risk model adopts model elements and relations between elements from the models of Stølen et al. (2002), Matulevicius et al. (2008) and Innerhofer–Oberperfler and Breu (2006). It uses rectangles for elements and arrows with a text annotation to describe the relationships between the elements. It adds elements for assurance, business requirements and business process modelling which are not present in the existing models. The

labelled arrows between elements like vulnerability and risk are added to describe the context of the relations and to make explicit the relations between the concepts related to risk, risk treatment, assets and security requirements. Labels are used to describe the connections between the elements. The core definitions of the model elements were described at the beginning of this section.

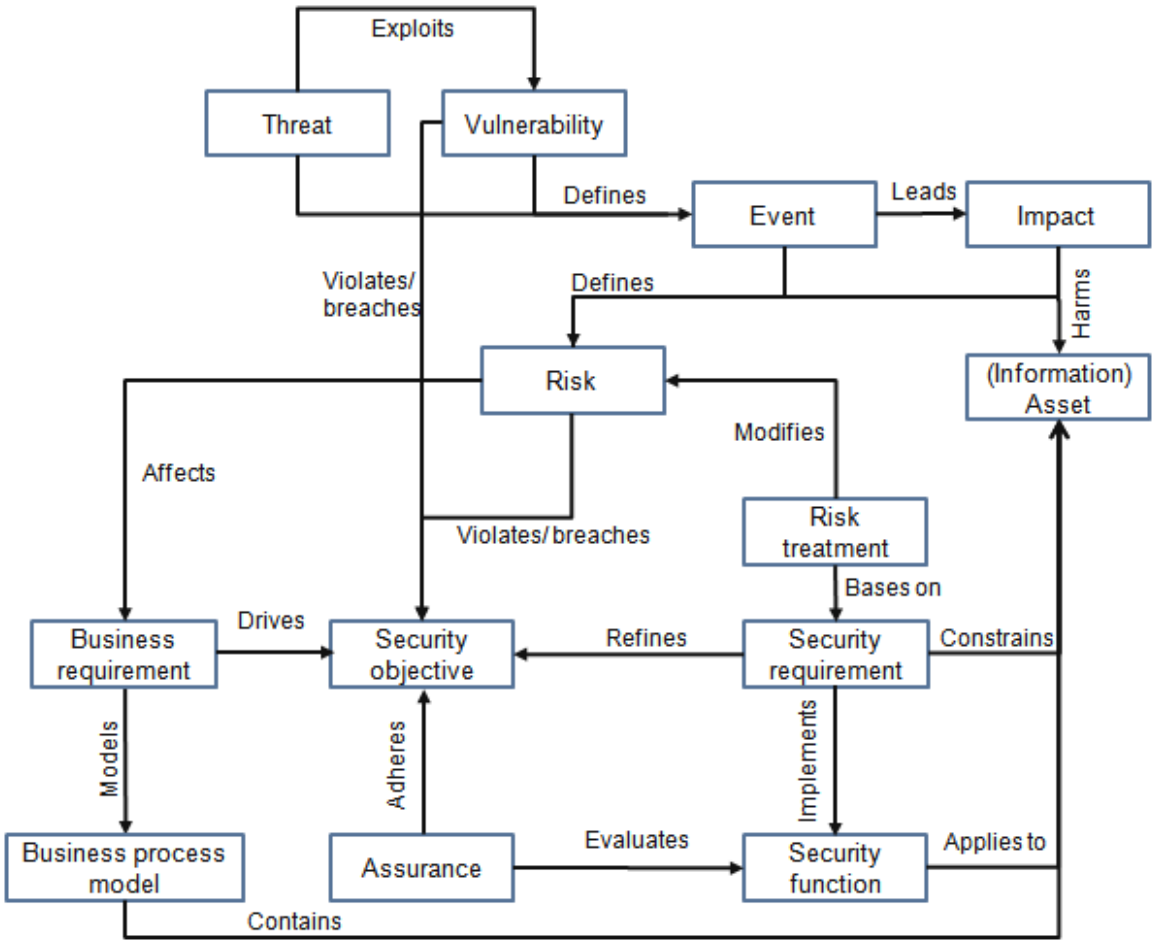


Figure 4-1 Extended information security risk model

Benefits of the model for research

In comparison to the existing models, this extended information-security risk model provides a combined view on concepts related to risk, risk treatment, asset and security requirements, similar to the model of Matulevicius et al. (2008). The difference is that risk treatment and asset-related concepts are related via risk *and*

security requirements, not only via risk. Model elements like risk, vulnerability, security objective, security requirements, security control and the asset are related, showing that risks and vulnerabilities have an effect on security objectives, security requirements and assets. Matulevicius et al. (2008) do relate risks to security objectives and requirements, but they use that relationship to indicate that security requirements mitigate risk and that the significance of risk is determined by the security criterion. Innerhofer–Oberperfler and Breu (2006) relate threats to security requirements. This indicates the violation, but it misses the links between security requirements and security controls, and their model also omits the concept of vulnerabilities. In the model of Stølen et al. (2002), vulnerabilities and assets are related via the security policy with security requirements, but risk treatment concepts are not made explicit. Because the extended information security model shows the effect of risks and vulnerabilities on security objectives, security requirements and assets, it can help to better understand the relationship between risk-, asset-, security requirements- and risk treatment-related concepts, and thus to achieve a better integration of these concepts within current risk assessment approaches. Furthermore, it is used as a foundation for defining risk in terms of security requirements - because of the relationship between risk and vulnerabilities, to security objectives and associated security requirements - rather than just in terms of threats and vulnerabilities.

4.2. Security requirement definition of risk

The extended information security risk model is the basis for the definition of risk in terms of security requirements. In the following a risk definition is developed based on the relations between risk, vulnerabilities, security objectives and requirements.

Risks and vulnerabilities violate the security objectives derived from business requirements, as the confidentiality, integrity and availability of information is not ensured. This can cause harm to the organisation. In the extended information security risk model, this is depicted as a relation with the labels “violates/breaches” between the risk or vulnerability and security objective. If the security requirement is not implemented, or not implemented correctly or adhered to, there is a negative impact upon the security objective, and ultimately also on the business requirements. This is because the security requirements refine the security objective defining the requirements for ensuring confidentiality, integrity and availability of information. Therefore, the non-adherence to security requirements is expected to harm the organisation and therefore constitutes a security risk.

The relation between a risk or vulnerability and a security objective is that the former can violate the security objective, refined by security requirements and implemented via security functions, thereby harming the organisation. Therefore, risk can also be defined as “the non-adherence to security requirements thereby causing harm to the organisation”. Hence, both a risk and a vulnerability can be identified by a deviation from or non-adherence to the security requirement by implemented security functions. Security functions are implemented by administrative, physical, and technical controls that fulfil security requirements. This means that correct implementation and operation of security functions with regard to the adherence of security requirements is key in order to prevent the organisation from being at risk, as well as for identifying risks and vulnerabilities.

4.3. Business process model information

A business process model is a detailed description of a business process including activities, agents, artefacts and roles involved in a modelling notation. Process activities describe what has to be performed by the process participants - or agents. An agent can be a human or system performing an activity. An artefact is a product that was created or modified by performing a process activity. A role is a set of activities that was assigned to process participants to define a functional responsibility. Business process models describe the value-generating processes of an organisation and can be seen as the place where risk materialises, information is generated and security functions are carried out, according to Rikhardsson et al. (2006). Therefore, business process models can be used to evaluate risks, vulnerabilities and security functions describing the operation and core values of the organisation.

Zur Muehlen (2005), who addresses risk management in the context of business process management, clusters business process model elements into goals, structure and information technology, data and organisation, according to his business process taxonomy (see Figure 4-2). The ‘goal’ cluster contains the purpose or objective of the processes that should be achieved. The ‘structure’ contains the activities of a process as well as the pre- and post-conditions necessary for the activities. The ‘information technology’ cluster contains the systems (i.e., applications as in the process taxonomy, networks, servers) and embeds the ‘data’ cluster, containing business objects which are processed at process activities. All these clusters are associated by relationships between their single elements. But only the process activity element connects all clusters -

besides data, which is embedded in the information technology and organisation cluster.

Because of these cluster relationships, the key to identifying risks and vulnerabilities with business process models is the process activity and the business object (data) of the business process. This is because the process activities describe the activities which have to be performed by process participants invoking systems, in order to achieve the business process goal. If a single process activity in a process is not performed on time and correctly then the process goal and ultimately the company's objective are at risk. In addition, the business object of a business process is important as it represents an information asset. The information asset has to be available and correct in order to achieve the objective of the process efficiently. Therefore, the availability, integrity and confidentiality of the information asset - set by the process objective - are crucial to the organisation's operations and are values to be protected by the organisation. Because of this, business process model activities and information assets are used in the proposed security requirement risk assessment approach.

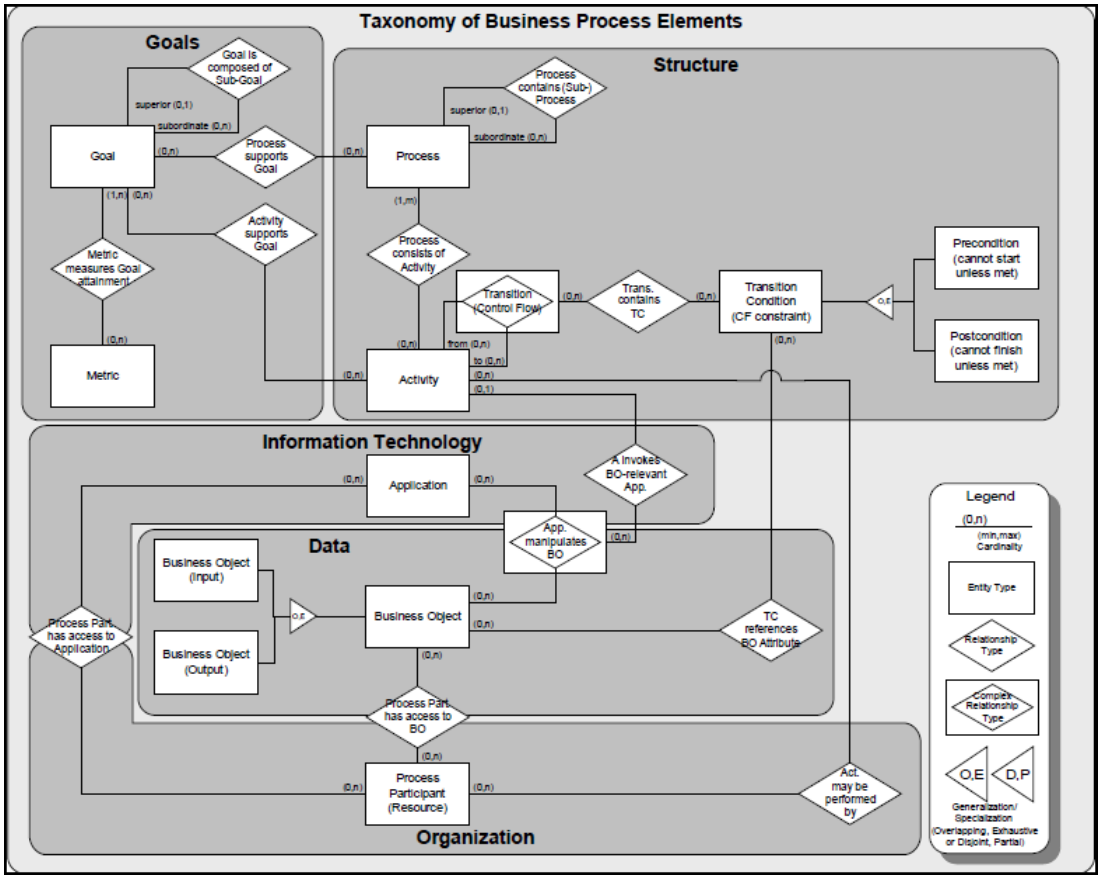


Figure 4-2 Business process taxonomy from zur Muehlen (2005)

It can be presumed that the quality and availability of process models in companies are sufficient to justify their use for information security risk assessments. Laws and regulations for financial service providers in the US and European Union require the identification of controls in the business context and solvency capital for risks, e.g. SOX (Sarbanes-Oxley Act, 2002); Basel II (Basel Committee on Banking Supervision, 2004); and Solvency II (European Commission, 2007). Process models contribute to identifying risks and controls, as they are often used as a basis to understand process activities and their associated risks, as well as to determine risks and/or control deficiencies within the analysed processes. Furthermore, the BPM surveys of 2008 and 2010 about current practices (Harmon and Wolf, 2008; Harmon and Wolf, 2010) confirm that

process models are available and up-to-date in about 55% of companies, as observed in these global market surveys which were answered by 264 respondents. In the survey among security professionals performed in 2011 (see chapter 3.4.2) it was also observed that business process models for critical and important processes in companies are both available and up-to-date.

4.4. Security requirements and business process models

In the following subsections, the utilisation of the concepts in a security requirements-based risk assessment approach on business process models is illustrated. First, it is highlighted why security requirements should be used to determine risks. Then, the relation and utilisation of the concepts used - security requirements, information assets and business process models - within a security requirements based approach are explained. Finally, the target of evaluation - business process activities and information assets - in the business process model is explained, together with how this model information can be used in the assessment.

4.4.1. Determining risk

In section 4.2, a security requirement based definition of risk was proposed, where security requirements are the basis for determining risks caused by vulnerabilities to a deviation or non-adherence. A vulnerability can be described as a weakness that can be exploited by an attacker (Stoneburner et al., 2002b). But, a vulnerability has to do with the security requirements of the evaluated target. This is the case because the weakness of the asset that constitutes a vulnerability has to be an inadvertent weakness. This implies that the weakness could be by design, and therefore is not really a weakness (when the requirements constitute this,

even if they are imperfect from a security best practice viewpoint). The same is true for the impact of vulnerabilities; the impact on an organisation is related to the (security) requirements and any (monetary) thresholds. Whether the impact has adverse effects upon the organisation depends on the security requirements refining business requirements in terms of security, as well as any security functions that are in place. Security functions - administrative, physical, and technical controls - can be processes that detect or prevent any events when an exploitable vulnerability exists; they can also serve to reduce the impact of these events. As a result, without determining and considering the security requirements and evaluating the security functions in place, no judgement about vulnerability and impact can be made. But if a security requirement is not adhered to - by a security function - the company would be at risk, as the security needs are thereby not fulfilled. ‘At risk’ means that a vulnerability exists and violates the security requirement, potentially causing harm to the organisation. Because of the reasons given above and the security requirements definition of risk, security requirement evaluation can be used to determine risks and vulnerabilities in a security risk assessment. Security requirements are the reference for defining the required security and determining whether a given vulnerability is a risk for the organisation.

Another aspect of security requirement evaluation and determining vulnerabilities accurately in risk assessment is the true value. If one would like to ensure the determination of all relevant vulnerabilities in a risk assessment, one would need to have a true value. The accuracy of a measurement system is defined as the degree of closeness to its true value (Viera and Garrett, 2005): this value can be defined as the adherence to security requirements, because such requirements specify the security needed as well as whether or not a security issue is a risk. The

degree of closeness to the true value cannot be indicated by current risk assessment approaches - methods used, such as security testing for vulnerability identification, only prove the presence of vulnerabilities, not their absence (Wang, 2005) - with regard to the security needed. As a result, a statement about the security of information or an organisation cannot be made. If the true value is used for vulnerability identification, the presence and absence of security vulnerabilities can be determined. In this thesis this would constitute the evaluation of security requirements and security functions being able to provide a statement about the security of information assets - thus resolving vulnerability identification errors.

4.4.2. Correlations

The extended information security model of section 4.1 describes the relationship between risk- asset- and security-related concepts, by elements. On the basis of the extended information security model, risk is defined as non-adherence to security requirements. Business process models are identified as being useful to determine risk (see section 4.3), as they describe how the business value is generated in processes and the place where risk materialises. Hereafter, the correlation between business process models and security requirements is illustrated; this is then utilised in the proposed security requirements risk assessment approach in this thesis. A correlation is a mutual relationship between model elements. These correlations between elements can be due to their definition, e.g. a security function is implementing a security requirement, or due to their usage, e.g. within process models assets and actors are modelled that use information assets. Figure 4-3 shows, by an arrow and a text annotation, the correlation between business process models, security requirements, information

assets and security functions. The arrow specifies the correlation to a related concept. Next, the correlations between these elements are explained.

A business process model contains information assets. Within a business process, information is processed to achieve the objective of the process. Information is used by the actors (e.g. humans) and the systems (e.g. an application or network) of the process, as such information represents the business transaction. Information assets have security requirements in order to ensure that the process objective can be achieved. The security requirements of the information asset are dependent on the business process objective, the context and the significance of the information relating to a company, product, service or person and represent a constraint. Security requirements are implemented via security functions for an information asset. Security functions afford protection in terms of the confidentiality, integrity and availability of an information asset. Security functions such as authentication mechanisms ensure that the security requirements of information assets are adhered to.

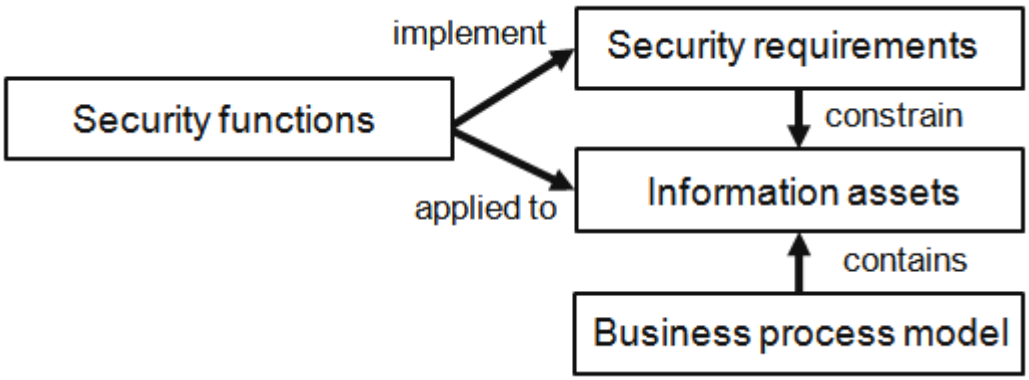


Figure 4-3 Correlation of concepts

Information assets are the key, as they connect business and security objectives by their requirements; security functions are applied to them, as well as being processed in the business context. The correlation between information assets,

business process models, security requirements and security functions could be used in a risk assessment to determine vulnerabilities. Security requirements can be evaluated by the security functions applied to the information asset. The information asset's security can be evaluated in the business process context by the process activities of value-generating processes where the information is used. By using these elements in an assessment, one can assure that the required security can be implemented, and that the organisation is not at risk.

4.4.3. Evaluation

In the proposed security requirement risk assessment approach, the correlations between the elements security requirements, information assets, business process models and security functions are used to identify vulnerabilities. Next, it is explained (with the help of Figure 4-4) how security requirements, information assets, business process models and security functions are used in the security requirements risk assessment approach. The circle with numbers in the figure indicates the relationship or concept that is used, as well as the sequence of their usage.

Initially, information assets are extracted from business process models (no. 1). Information assets can be identified by the information used in the process activities of critical business processes. Information assets have security requirements that can be defined for them, and as such represent constraints (no. 2). For the definition of security requirements, artefacts such as business process objectives and security objectives, security policies or security best practices can be used. These security requirements of information assets are analysed and evaluated, in process activities of the business process model (no. 3), in respect of implemented security functions applied to information assets (no. 3), so as to

determine vulnerabilities. In each business process model activity, where information assets are used, the asset's security requirements are evaluated to determine whether the implemented security functions fulfil them.

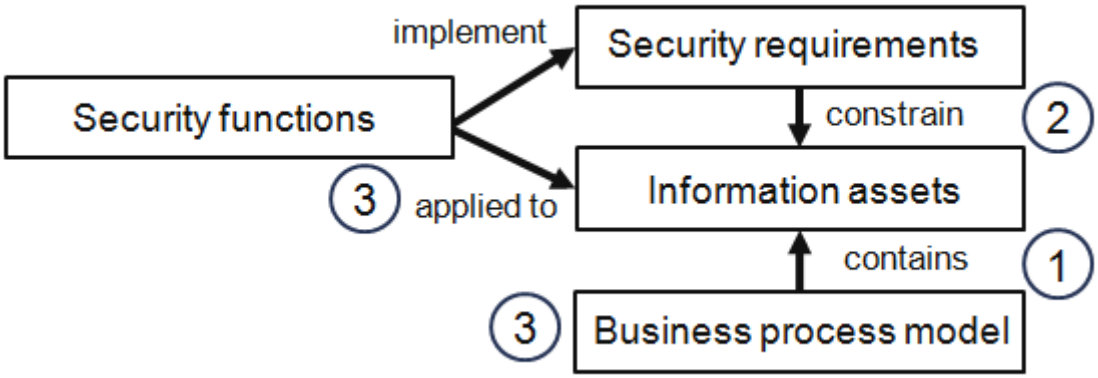


Figure 4-4 Utilization of concepts

The advantage of evaluating information assets' security requirements with a business process model is that the basis for evaluation - security requirements representing the true value - is defined and explicitly evaluated in the operational business context. A statement about the security of information assets could be provided by the processes' and information assets' risk results, which show only true positive vulnerabilities. This statement can be provided as not only vulnerabilities are determined, but also the security needs are identified together with whether or not they are fulfilled. As a consequence, security design and security operation vulnerabilities (for example) can be determined more accurately rather than being based simply on security best practices for a single asset. Furthermore, security (inter)dependencies between information assets or processes (see 4.5.3) can also be considered, as the evaluation is performed systematically on security requirements of information assets, in the course of business. The difference to other approaches - which use parts of business process models, information assets or security requirements - is that vulnerability

identification for an information asset is based on the asset's explicit security requirement evaluation, by considering business process activities and the implementation of security functions.

4.4.4. Target of evaluation

In the section above it was outlined how concepts like security requirements and business process models are applied in a security requirements risk assessment. In this section, the utilisation of business process model information - in particular, process activities and information assets - for determining security risks and vulnerabilities is described. Process activities can be used as the *target of evaluation* in an assessment, and the process objective and information asset to determine the *criticality* of occurring risks.

To determine the *criticality* of a process, one can use the process objective and any input or output - the information asset representing the business transaction - of a process and its associated activities. The business process objective and the information asset can help to assess the impact for the organisation, and if the process is impaired. For example, using an impact evaluation of whether or not the business objective is achieved or only partially achieved, as well as the criticality for the organisation and its mission can be determined. Furthermore, the information asset processed can also be the input for other processes, to indicate how critical any corruption or leakage of the information (or interruption of the process) would be for the organisation. The impact can be determined quantitatively, if possible, or qualitatively.

Secondly, the processes cluster referred to as structure, information technology, data and organisation in the process taxonomy of section 4.3 can be used as the *target of evaluation* in an assessment. The clusters and their related vulnerabilities

- such as security design-, technical-, security behaviour- and information processing issues - can be identified by evaluating process activities. This is because the process activities are associated to the clusters by describing the interactions between, and usage of, clusters (see section 4.3). Typically, process activities describe the manipulation of the information asset, the process participant who is performing the task and the system used, e.g. applications, networks, servers, etc. They can all be used as targets of evaluation representing the clusters. But in a process, multiple process activities are available which process the information asset and describe the information asset's flow within the process. Therefore, one can distinguish between the *processing* of information and the *process elements* handling the information, within a business process. With *processing*, the processing of information assets relating to the different activities of the process is meant. At these processing points, information assets are created, processed, and communicated. With the evaluation of these processing points the security related to access, manipulation and communication of information assets can be determined, as well as whether the process design from an information flow perspective is secure. At each process point, the implemented security functions can be evaluated based on the information asset's security objectives. The *process elements* are the systems and process participants relating to the process activities that handle the information asset. Process elements can be described as containers handling the information assets in the process activities. Containers can be any type of system (applications, networks, servers, etc.), a process participant (a human or machine) or the environment (an organisation or facilities) in which the information resides. The reason why the processing of information and the process elements are differentiated is that the process elements themselves can have a weakness,

which might be a risk for the information asset, although unrelated to the processing of the information asset and vice versa. Therefore, the security of information assets is determined by the security of *processing of information* and the security of *process elements*.

Furthermore, the security of information assets is also dependent on *security processes* that, for instance, grant the process participant process activity access to information or a security process, such as the patch management process. These security processes are about the operation and maintenance of process elements, and should ensure their security. If one of these processes fails, the information asset is vulnerable; the process element might not be adequately protected, resulting in a vulnerability. Therefore, security processes have to be included in the evaluation of process elements with regard to their security. With the evaluation of the process elements and the IT security processes, technical-procedural- and behavioural issues can be determined, as well as the capability of the processes to protect assets from security issues. The IT security process evaluation determines any weakness to protect assets from security issues in the operation of process elements.

To conclude, the security of information assets within a business process is determined by the *processing of information* in the process activities and the *process elements* handling the information, as well as the *security processes* managing the operation of process elements. Hence, to assess the IT security risks of information assets with business process models, one has to assess the security of information in the *process elements* handling the information - containers of information assets - the *processing* (information flow level) *of information* in the process activities, and the *security processes* ensuring secure operation. The *processing, process elements and security processes* -

representing the targets of evaluation - should be considered in a security requirement risk assessment. This will also form the basis of the security requirements characterisation structure proposed in section 4.5.2.

4.5. Defining security requirements

In the following subsections, firstly the security requirement elicitation process is discussed and secondly a security requirement characterisation structure based on business process information is proposed. Thirdly, it is illustrated that through the evaluation of the information assets' security requirements, dependencies can be considered in a risk assessment.

4.5.1. Elicitation

Existing information security risk assessments that use security requirements propose neither a formal process as to how to elicit security requirements, nor a structure for defining them. They define them as text for: model elements of the organisation's architecture (Breu and Innerhofer-Oberperfler, 2005); assets (Stoneburner et al., 2002b); or scenarios (Caralli et al., 2007). In software engineering (SE), different approaches have been proposed for security software engineering, containing activities for the definition and elicitation of security requirements. However, these approaches differ in the extent of the process steps as well as the starting point of the elicitation. For example, Square (Mead et al., 2005) starts with security goals and ends with requirements' inspection in nine process steps; Haley et al. (2008) start with functional requirements and end with system verification in four process steps; and Boström et al. (2006) start with critical assets and end with checking abuser stories and countermeasures in seven process steps. Tondel et al. (2008) surveyed the literature for security

requirement elicitation techniques and compared these security requirement engineering approaches based on the elicitation process steps. They conclude that there is no common definition of process steps, and that the different approaches don't agree on what a security requirement is and whether concrete security measures should be specified. As there is no universally accepted definition of security requirements or of the process steps for security requirement elicitation, either in risk assessment approaches or at security software engineering approaches, the following process steps are defined for the elicitation of security requirements based on Tondel et al.'s proposal:

- Identification of assets - critical processes and their information assets are identified;
- Identification of security needs and legislation, policies, standards and best practices that apply to the process including actors, activities and information assets;
- Definition of the security objective (SO) level and security requirements (SR) for information assets, based on identified security needs;
- Checking for consistency and dependencies of information assets at SO and SR, by using one information asset requirement definition at all business processes.

The security requirements elicitation process above differs slightly in the third step of definition of security objectives and requirements. Tondel et al. (2008) suggested that a risk analysis is to be performed; and in the information security system risk management process of Mayer (2009), a risk assessment is also to be performed. In these approaches, security objectives are defined first. Then a risk analysis/assessment is conducted to determine threats or vulnerabilities and then

the security requirements identified. Contrarily to the proposed security requirement elicitation steps discussed previously, one can argue that to determine security requirements, security knowledge about events (the combination of threats and vulnerabilities), the impact of the events and the effect of measures are all necessary; these would be determined in a risk analysis/assessment. However, in this thesis, it is argued that this elicitation step is not imperative. The following example of a threat and vulnerability should illustrate this. Wireless data transmissions without encryption can be intercepted and easily read by a malicious user. The fact that wireless data transmissions can be intercepted as well as read, if no encryption is provided, must be known by the security expert or be present in a security knowledge base. But, this knowledge is already explicitly available in public media, at security conferences and in security standards. This knowledge is not determined explicitly in a risk analysis/ assessment; it is only determined as to whether the system is vulnerable to this issue. Current risk assessment approaches identify known vulnerabilities by using best practices relating to security, as well as knowledge bases, but they don't identify new and as yet unknown vulnerabilities. This explicit universally valid knowledge (that is generally available and accepted by the public) is also used in the security requirements definition in the proposed elicitation steps. The instance of wireless data transmission is an example of such knowledge that wireless data transmissions should be secured, for instance, by encryption measures representing the security requirement. The argument that security requirements cannot be defined as they use risk assessment knowledge - specifically relating to a system's vulnerabilities that are determined in a risk assessment - is not valid, as the security requirement should describe what is to be protected and not merely provide a security statement of a system's existing vulnerabilities. To describe

what should be protected, explicit security knowledge can be used with regard to the business security needs and the potential causes of harm to the business. Therefore, a risk assessment is not imperative.

Basically, for the security requirements definition, the same basis of security knowledge is used, as for vulnerability identification in risk assessments. In contrast to current risk assessment proceedings, the necessary security is defined beforehand, and in the risk assessment how the implemented system should be is verified - against the design and operation - in order to identify vulnerabilities. In existing approaches, vulnerabilities described in knowledge bases are compared with the current situation, and don't consider how the system should be. To evaluate how already existing systems should be - their security requirements - it is necessary to define the security requirements prior to the assessment; this is different to software engineering where systems are developed based on the security requirements. Therefore, in this thesis, the security requirement elicitation process differs from software engineering and it is proposed to specify security requirements without any risk assessment.

4.5.2. Characterisation

To specify security requirements, as well as for them to be utilisable in a security risk assessment with business process models, they have to be documented in some form. Security requirements should be characterised in a way which is understandable by the business user for verification purposes; it should be light-weight and it must be usable by a security expert, whilst also being capable of elicitation without necessitating any additional knowledge or modelling. Ideally, security requirements are characterised by a structure aligned with the business context - the security needed in the operation - and no additional information or

modelling should be necessary. This is because the security requirement structure should help to assess them correctly and efficiently, and should provide a measurement criterion. In current risk assessment approaches that use security requirements, the requirements are described, e.g. as textual annotation for a scenario (Caralli et al., 2007), as a modelled element of the enterprise architecture (Innerhofer–Oberperfler and Breu, 2006), or as a checklist (Stoneburner et al., 2002b) for an asset. In these approaches, security requirements are specified as text for an asset or element with regard to confidentiality, integrity and availability. But these textual specifications are neither structured to support the assessment process with business process models - they are instead attached to an element - nor are they reusable within other processes or process activities. Security requirements should be specified for an information asset in order to be (re)usable in other processes or activities. They should also consider the processing and handling of information (see section 4.4.4) in order to assess them efficiently and correctly, as discussed above. As in software engineering, modelling notations and frameworks were proposed to model security aspects as well as to derive security requirements (see section 3.2.2.). There may be approaches which are utilisable for security requirements' characterisation that fulfil the previous requirements. Therefore, a few software engineering modelling notations of section 3.2.2 are examined to determine which approach might be best to characterise security requirements for information assets of business process models, as relating to the identification of vulnerabilities.

Problem frames (Jackson, 1999) are an approach aimed at specifying user requirements for software. They decompose user requirements of real world problems. Cox and Phalp (2003) describe how to generate problem frames out of

business process models for the usage of process knowledge relating to the requirements phase. Cox and Phalp derived problem frames but ran into problems; such as problem frame domains not always being apparent. Also, information might be lost, or it may be necessary to specify other frames. Cox and Phalp worked with role activity diagrams (RAD) but do not reveal experience with other business process notations. In addition to the issues found by Cox and Phalp, no additional criteria for security requirements or evaluations can be specified.

An attack tree (Schneier, 1999) provides an overview of attacks and shows how to achieve the attack goal - the root of the tree. It is presented as a tree structure consisting of the attack goal as the root and the sub-attack goals as branches. Leaves of the attack tree are attacks to achieve sub-attack goals. Attacks and sub-attack goals can be performed in combination; this is represented by the nomenclature “And”. Attack trees can be used to specify security requirements but do not facilitate the specification of requirements. This means that out of the attack tree, one has to elicit and interpret the security requirements for the asset based on the attack and attack goal. Furthermore, the attack tree does not provide any structure showing how to define the security requirements.

A misuse diagram (Sindre and Opdahl, 2005) presents the mapping between the use and misuse cases, via threat mitigations. A misuse case is the inverse of a use case and describes functions that should not be allowed and would result in a loss for the organisation or a stakeholder. The graphical representation helps to analyse and elicit security requirements. To use misuse cases for security requirements, there is a need to identify and model use cases, misuse cases and threat mitigations. The threat mitigations or safeguards represent the security requirements for information assets in a particular use/misuse case. Use and misuse cases describe security requirements specific to a particular case and one

would have to determine how the security requirements for the information assets and systems relating to different use/misuse cases have to be documented further. This means that all the security requirements have to be collected and documented within some kind of structure to be used for the security risk assessment; this creates additional efforts besides the modelling of the cases.

An abuse case is a specification of an interaction between a system and an actor wherein the results of such an interaction are harmful to the system, the actor or the stakeholder (McDermott and Fox, 1999). Abuse cases are described with the same notation and symbols as use cases. When creating an abuse case, it has to be both identified and defined. Abuse cases can help to determine and elicit security requirements. But to draft abuse cases, one has to be aware of possible threats and vulnerabilities. Further on, an abuse case provides no specification structure or scheme for security requirements of assets.

With semantic data models, the security requirements of data can be modelled to describe the constraints between data (Smith, 1990). With this approach, the dependencies of data entities relating to integrity and secrecy can be presented. However, it requires knowledge about the data structure that is either not available in or cannot be derived from, for instance, a business process model. The semantic data model would always be incomplete and does not include anything relating to the specification for security requirements.

Wang and Wulf (1997) propose a framework for security measurement to approximate the security strength of a system. Because the security objectives are often only available in qualitative terms, they use a factor criteria model to specify the security objectives more definitely, in order to measure them against these criteria. For example, confidentiality is divided into three main factors: software access control, physical security and cryptographic protection. These factors are

further divided into a set of criteria, such as reliability and effectiveness for software access control. Then, a measure is defined for a criterion or further sub-criteria. The underlying concept of the factor criteria model - decomposition of elements - is used both to specify security requirements as well as to evaluate the corresponding security functions.

Security requirements for information assets

If business process model information is used for a risk assessment, then ideally the security requirements characterisation should be aligned with this information to be understandable in the context. A textual annotation for a security requirement specification, as used in current information security risk assessment, without any structure or assigning security requirements to single assets being able to reuse them and supporting the assessment would not be efficient in describing them for the evaluation in a business process context. The factor criteria model proposed by Wang and Wulf (1997) would help to measure security more definitely; it would also provide a structure for the definition of security requirements, but is not aligned to business process model information and evaluation. On the other hand, this alignment between the security requirement and the business process context is necessary, as an information asset security requirement has dependencies on other applications, process participants or security processes. Because security requirements can be different to the applications context (Haley et al., 2008) they must therefore be checked with regard to consistency, completeness and redundancy over processes.

In section 4.4.4 *processing* and *process elements,* referred to as containers and their *security processes,* were identified as targets of evaluation of a business

process model. Therefore, for the security requirements structure and to support the evaluation process, decomposition and the idea of a factor-criteria model (Wang and Wulf, 1997) have been applied as follows. Security requirements are defined for an information asset at each of the levels - processing, containers and security processes. The processing security requirements of information assets are defined by a security objective rating, which is used because information assets can be processed in different business processes, process activities and process elements, making it difficult to define a specific requirement. The security objective rating for processing of an information asset is evaluated via a predefined set of security functions defining the security requirements alike in a factor-criteria model. A predefined set of security functions is used as otherwise there might be misinterpretations of how to evaluate confidentiality, integrity and availability (Wang and Wulf, 1997) in the context. The evaluated security functions are “access control & accountability”, “authorisation”, “data input validation” and “encryption”. Process elements are defined as containers handling the information asset (e.g. systems or humans are defined as process participants) or where the information asset resides (i.e. the organisation or facilities). The container security requirements and IT security processes are described in natural language, because these requirements are specific to the container and cannot be generalised. The container security requirements are decomposed into ‘primary systems’, ‘organisation/people’ and ‘environment/physical’. These three categories follow the characteristics of a process activity - process participants either use systems or interact with their environment - and should help the assessor to evaluate the business process activities efficiently and with less interpretation of the adherence to the security requirements. Furthermore, IT security processes for the containers have to be defined as discussed in section 4.4.4. These security

processes ensure and operationalise security for ‘primary systems’, ‘organisation/people’ or the ‘environment/physical’ on which they are dependent. Best practice security processes can be used based on standards like COBIT (ITGI, 2007) or ISO17799 (ISO, 2005c) to specify security processes for the containers’ security requirements. Technical vulnerabilities and IT operation issues should be identified with the assessment of these IT security processes, because these processes are mainly about the operation and maintenance of systems. Furthermore, the evaluation of IT security processes can support the results “independent of a point in time”, in the knowledge that risks do change over time (Jackson, 2007), and the security of information is dependent on the capacity to handle or prevent/limit risks in the near future. IT security processes can also be evaluated with regard to maturity and performance using, for example, an existing maturity model like CMMI (Paulk et al., 1993) to provide a statement about the capability of the processes to detect and prevent vulnerabilities. The result of such a security process assessment would strengthen the result statement for the asset or organisation, as it would indicate how well the current security state can be maintained in the near future. The security requirements characterisation structure shown in Table 4-3 defines the security needs of an information asset, considering the processing of information, the containers handling the information as well as security processes needed for the containers.

Table 4-3: Security requirements for information assets

Information asset:		**Integrity**	**Confidentiality**	**Availability**	**IT Security Processes**
Processing	Data	Integrity, Confidentiality and availability security objectives rating.			n/a

Containers	Primary Systems	Integrity, confidentiality and availability requirements for the systems that processes information.	IT security processes that ensure the security of systems.
	Organisation People	Integrity, confidentiality and availability requirements for the actors or the processes that handle the information.	IT security processes that ensure security in the organisation.
	Environment/ Physical	Integrity, Confidentiality and availability requirements for the environment where the information is physically available.	IT security processes that ensure security for facilities and the workplace.

4.5.3. (Inter)dependencies

Security requirements for an information asset describe the functional requirements or constraints (Haley et al., 2008), affecting one or more systems in the processes where the information asset is used. Dependencies or interdependencies can be observed between processes and systems and their information assets security requirements, as they all use this particular information asset. An interdependency can be defined as “a bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other” (Rinaldi et al., 2001, p. 14), and a dependency as “a linkage or connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other” (Rinaldi et al., 2001, p. 14). The difference between an interdependency and a dependency is whether the link is bi- or uni-directional. Interdependencies or dependencies in security - in contrast to in safety - are related to the security principles contributing to confidentiality, integrity and availability of information. Segregation of duties, access control, authorisation, accountability and authenticity are examples of such security principles. As an example, a process or system relies on information (e.g. timeliness, integrity, availability) of another process or system, on the security (e.g. public key infrastructure, access control) of another process or system, or on the

availability of another process or system. These interdependencies or dependencies between processes or systems can be physical (availability of goods, personnel, etc), technical (e.g. operability of a web based service), functional (e.g. usage of materials or services that are within the specification) or conditional (e.g. triggers as used in supply chains or integrity of information). This means that the output of a process or system can be dependent on a state that is not within the process or system considered. For example, Research and Development (R&D) information can be secure in the R&D department or related R&D processes. However, it might not be secure if it is used in the marketing department or marketing processes, as applied security functions may not adequately protect this kind of information. In this case, the security of information with regard to its publication or leakage is dependent on corresponding security functions of the process. Vulnerabilities might exist - and might not be detected - if these kinds of interdependencies or dependencies between processes, systems and information assets are not considered in the information security risk assessment.

Implications for security risk assessments

According to ISO 27005 (ISO, 2011c), dependencies should be considered in the asset valuation step to determine the asset's value. However, considering dependencies in the evaluation process is not described or elaborated in ISO 27005. Furthermore, in current assessment approaches, security requirements are evaluated only for single assets or best practice security requirements used, but with this, interdependencies or dependencies cannot be fully taken into account. This is because security requirements are not evaluated in the context of the processes where the information asset is used. Therefore, the information asset's

specific security requirements have to be evaluated in the systems, over communication channels (network and internet, for example), as well as in the processes (company internal or external) which use that information. This procedure allows for considering of the dependencies and interdependencies; the asset's security requirements are evaluated in the different systems where it is processed. In contrast, current security risk assessments do not address the interdependencies or dependencies of an asset's security requirements. Security requirements and security functions are not evaluated for multiple assets, but rather vulnerabilities of assets are determined.

4.6. Chapter summary

In this chapter, the extended information security model presented shows the relationships of vulnerabilities and risks between security objectives, requirements and assets. Because of these relations, security requirements can be used for the identification of risk and vulnerabilities for an asset, with regard to both the security needed and the implemented security functions. A definition of risk based on security requirements was provided as being necessary to determine risk using security requirements. By this definition, security requirements can be the basis for identifying risk and the resolution of vulnerability identification errors; they have a relation to vulnerabilities, risk, security controls and assets and provide a measurement criterion - the security needed - for risk. Security requirements not only form the basis for identifying vulnerabilities of information assets, they can also be used to indicate the security of information - whether security issues are present (by identifying vulnerabilities) or absent (by verifying security needs and corresponding security functions). Actually, this would allow for making a statement about the security of information.

Furthermore, the mutual relationships between security requirements, business process models, information assets and security functions were presented and illustrated, together with how to apply them to determine risks and vulnerabilities. It was also explained how business process model information can be used for risk assessments, and that for the evaluation of information assets, processing and process elements (containers) handling information must be distinguished, and IT security processes operationalising security must be considered. This is because an information asset is accessed or manipulated by systems, as well as process participants, in multiple process activities. By ‘processing’, the communication or manipulation of information assets is meant; on the other hand, the word ‘containers’ is used to specify process participants, systems or the environment where the information assets are handled and where they reside.

Next, a security requirement elicitation process and characterisation structure was presented. This can be used for the security definition and evaluation of business process model information. The security requirement elicitation process omits risk analysis/assessment, because security requirements describe what should be protected rather than the system’s current vulnerability. The security requirements characterisation structure is defined for information assets considers processing and the containers of handling information in business process models, as well as IT security processes. In that sense, it follows the concept of decomposition and uses the idea of a factor-criteria model. By defining the information asset’s security requirements and evaluating them in business process activities, (inter)dependencies between business processes, process participants and systems using the same information asset can be considered.

Chapter 5 - A Security Requirement Risk Assessment Approach

This chapter presents the proposed security requirements risk assessment approach called ‘SRA’ for the identification of vulnerabilities with security requirements and business process models. The conceptional foundation for the approach - the relationship between security requirements and risk - is the enhanced information security model of section 4.1 and the security requirements based definition of risk of section 4.2. The SRA’s procedure is based on the concepts of business process models, security requirements and information assets, and their respective correlations as described in sections 4.4.2 and 4.4.3. The security requirements structure and evaluated elements of business process models is described in sections 4.4.4 and 4.5.2. The first section of this chapter will provide an overview of the approach, followed by a detailed description of the phases of the approach - in section 5.2 - and applying the approach to a running example in section 5.3.

5.1. Introduction

An information security risk assessment should consider both organisational and technological issues (von Solms and von Solms, 2005), providing a company-wide view of risk, both as a baseline for improvement and as a statement of security. By using business process models, one can consider organisational issues; by evaluating security requirements of information assets, one can identify technological issues as well as provide a statement of security. Information assets

can be described as information handled by systems or people residing in facilities of organisations. Such a security requirement risk assessment approach differs at the vulnerability identification phase to current proceedings, because information assets' security requirements are explicitly evaluated in the business context against security functions to identify risks, instead of by using a list of vulnerabilities or security best practices. The aim is to determine and resolve vulnerability identification errors on the basis of information assets' security requirements and business processes, rather than by identifying and evaluating vulnerabilities for single assets. This explicit evaluation of security requirements provides benefits, as business security needs and organisational issues are considered. The presence and absence of risk could thus be indicated by evaluating security needs; probability statistics and detailed impact estimates are not needed.

5.2. The approach

In the subsequent sections, each phase of the security requirements risk assessment approach (SRA) is explained in detail. The approach consists of six steps, organised into four phases, namely asset identification, asset profiling, vulnerability identification and risk documentation. Figure 5-1 shows the assessment phases and steps; a rectangle represents a step in the assessment process and the arrows indicate the order of the steps.

In phase one, 'asset identification', information assets (Stevens, 2005) are identified using business process models of the company's critical business processes. Events occurring in these processes would cause substantial impact to the company, as the business goal or objective would be endangered. Business

process models describe a structured flow of activities of actors and applications (systems that perform or support an activity), using information assets embedded in an environment (e.g. an organisation or facilities) (zur Muehlen, 2005). These information asset-representing business transactions can be identified by what information is used by actors or applications. The information assets are needed as an input for the next step - for the definition of security objectives and requirements. Phase one is completed when information assets are identified, however it does not necessarily require the identification of all assets at the first attempt - this activity can be restarted.

In phase two, ‘asset profiling’, security objectives and requirements are defined for each information asset. This profiling step establishes clear boundaries of the security required, with regard to the processing of information, containers handling the information asset in a process and security processes applied, as well as when a vulnerability becomes a risk. Security objectives can be defined as high-level descriptions of the security to be achieved, whilst security requirements are refinements of the security objectives as the constraints required for the system to be satisfied (Mead and Stehney, 2005). Artefacts that can be used include the company’s security policy, organisational procedures and security best practices. The verification of security requirements with regard to validity and correctness is not an aim of this phase. Any dependencies and inconsistencies between the security needs of information assets can be identified by defining and aligning the security requirements for different business processes in which the information asset is used.

In phase three, ‘vulnerability identification’, the information asset security requirements with regard to implemented security functions are evaluated on the basis of entry, process and communication points in the business process model. An entry, process and communication point is an activity by an actor or system in the process where an information asset is created, processed and transmitted respectively. With the evaluation of the asset’s security objectives at entry, process and communication points, the secure processing (entry, processing and transmission) of the information is determined. With the evaluation of the asset’s security requirements at the containers (systems, actors and the environment), the secure handling of the information is determined. Containers are systems, people or the environment utilising the information asset, or where information resides. In this thesis it is presumed that (see section 4.2) if security requirements are not implemented, not implemented correctly, or not adhered to, there is a negative impact upon the security objective and ultimately upon the business requirements and the organisation as a whole. Therefore, a risk and vulnerability can be identified by a deviation from, or non-adherence to, the security requirement by implemented security functions. Security objectives are evaluated by predefined security functions like access control or encryption, whereas security requirements instead by their implementation. The assessment is completed when all entry, process and communication points of the process are evaluated. Information asset identification can be restarted or applied iteratively (the arrow between steps 3.2 and 1.2), if a new asset is identified in the vulnerability identification phase.

In phase four, ‘risk documentation’, vulnerabilities and the information asset at risk is acknowledged for each business process. The assessment is completed by documenting the vulnerabilities and risks. For each business process and

information asset, a statement of the security can be provided by having or not having a vulnerability identified, where an information asset is either at risk or not at risk.

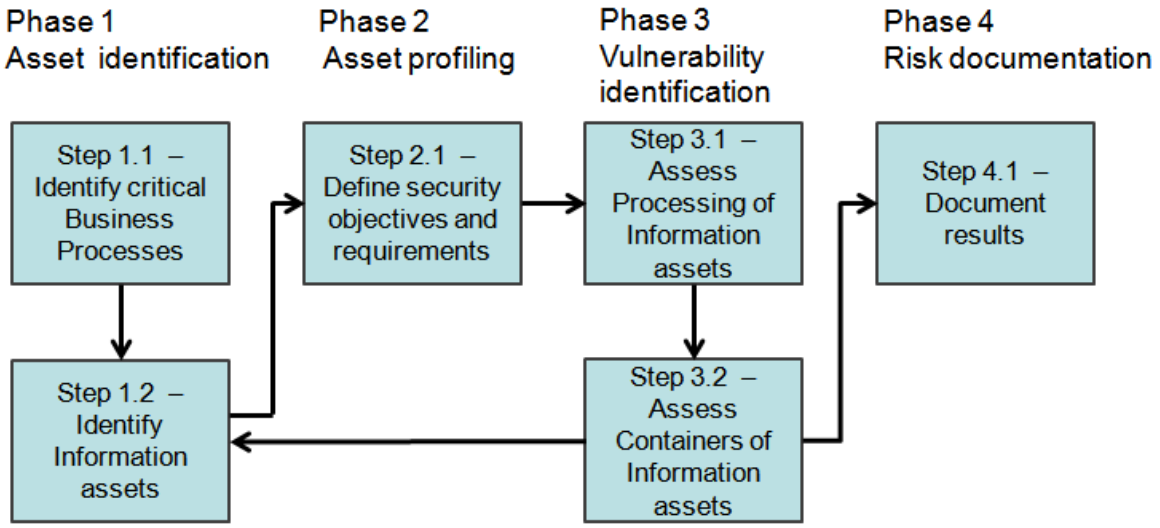


Figure 5-1 Security requirements based risk assessment process (SRA)

In the following, the different phases of the security requirements based risk assessment process (SRA) are explained.

5.2.1. Phase 1 - Asset identification

In step 1.1, the objective is to identify the critical business processes of a company and the information assets of these processes. The criticality of the business process can be determined by the objective and output of a process and its value for the organisation. For example, the required availability level for a process can be determined by the loss caused due to disruption of operations, or a business impact analysis - where critical functions of an organisation are identified whose disruption is regarded as unacceptable (e.g. a production process) - can be used. The required availability level should be evaluated in relation to all business processes at the company - assessed on the basis of the impact of a complete breakdown of the process - with a qualitative scale, e.g. high, medium. For

example, the Maximum Tolerable Downtime (MTD) could be used to determine the availability of the process.

In step 1.2, information assets representing business transactions have to be identified for defining security requirements. Criteria and indicators for identifying information assets are decision points and process activities. These information assets are naturally grouped (e.g. payment data) or are already grouped by process activities (e.g. order data) and can be identified by the process activity descriptions or process names. At a process activity, customer data or payment data is entered. Another example is the processing of contract, order or customer data.

5.2.2. Phase 2 - Asset profiling

In this phase, the security objectives and security requirements are defined for identified information assets labelled as information asset security requirements. For specifying the information asset security requirements, the security characterisation structure of chapter 4.5.2 is used in order to distinguish between processing and the containers of information assets. At the processing level, the security needs for the processing of the information are specified. These security needs for an information asset are defined as security objectives on the basis of a security objective rating. Implicit requirements may have to be considered, such as the necessity of complete and accurate information or explicit requirements for information to be protected under privacy laws. For information asset containers, security requirements are defined for a process' actors, systems and environment; the information is handled considering the security objective level. On both processing and container levels, objectives and requirements are defined for

integrity, confidentiality and availability, as well as IT security processes at container level. The elicitation of security objectives and requirements for identified information assets has to be conducted by the assessor based on security needs, legislation, policies, standards and best practices.

Security objectives for processing

At the processing level, the security objective for the information asset is defined on basis of a security objective rating for confidentiality, availability and integrity dependent on the information asset's criticality. In order to classify between security levels for a security objective, a rating was derived (see Table 5-1). To specify the security objective rating, one should identify security needs, relevant legislation, standards and policies that apply. The rating used for the information asset's security objectives is based on a qualitative scale with the following meanings:

Table 5-1 Security objectives' rating

Integrity rating	
Level 1 (Poor)	Information should be accurate but need not be complete.
Level 2 (Average)	Information must be accurate and complete.
Level 3 (Trustable)	Information must be accurate, complete and a person must be accountable.
Confidentiality rating	
Level 1 (Public)	Information access must not be restricted.
Level 2 (Internal)	Information access has to be restricted to people within the company.
Level 3 (Confidential)	Information access has to be restricted to single users.
Availability rating	
Level 1 (business days)	Information needs to be available within the next days.
Level 2 (24 hours)	Information has to be available within the next 24 hours.
Level 3 (Immediately)	Information has to be available instantly.

Security requirements for containers

At the container level, security requirements are specified for systems, actors, the organisation and the physical environment, as well as IT security processes designated guaranteeing the protection of the asset (see Table 5-2, third to last row). To define the security requirements, one can use artefacts like the company's security policy (guidelines, technical parameters, etc.), organisational procedures (e.g. procedures for installation, changes), and security best practices, such as the ISO 2700x series. The container security requirements refine the processing security objectives and describe what should be protected, as well as the concrete security function implementation. In addition, IT security processes which ensure and operationalise security (see Table 5-2, last column) have to be defined, derived from IT operation guidelines like ITIL (CCTA, 2007) or security standards like the baseline protection manual (BSI, 2008). Any detailed specification for IT security processes is not necessary within our information asset security requirements specification, because - for efficiency reasons - already standardised and internationally accepted security process definitions and their descriptions can be reused for the evaluation.

Table 5-2, below, shows the information asset security requirements definition for an information asset. Integrity, confidentiality and availability are rated on processing level and detailed specifically for containers. IT security processes are only specified for containers such as actors, systems and the environment.

Table 5-2: Information asset security requirements

Information asset: Customer data		Integrity	Confidentiality	Availability	IT Security Processes
Processing	Data	Integrity, Confidentiality and availability Security objectives rating according to the ratings specified.			n/a
Containers	Primary Systems	Integrity, confidentiality and availability requirements for the systems that processes information.			IT security processes that ensure the security of systems.
	Organisation People Process	Integrity, confidentiality and availability requirements for the actors or the process that handle the information.			IT security processes that ensure security in the organisation.
	Physical	Integrity, Confidentiality and availability requirements for the environment where the information is physical available.			IT security processes that ensure security for facilities and workplace.

5.2.3. Phase 3 - Vulnerability identification

At step 3.1, the degree of implemented security functions (activity one) at the processing level and their adherence to information assets security objectives (activity two) are evaluated. At step 3.2, the information assets' containers (i.e., systems, actors, and environment) and security requirements are evaluated.

Step 3.1 - Asses processing of information assets (activity one)

To determine the adherence to security objectives, implemented security functions are evaluated. But before security functions are evaluated, one has first to determine where the information assets in the process are created, processed and transmitted. These process points are defined as entry (EP), process (PP) and communication (CC) points. Entry points (EP) describe activities where information available is made processable by its entry into a system. Process points (PP)

describe activities where information is permanently saved electronically or modified (processed). Communication channels (CC) describe activities where information between process activities is transmitted. The information transmission can be across organisational borders, geographic locations or between departments. The EP, PP and CC can be identified by keywords (e.g. enter, save, send) of process activities' descriptions. Entry points, process points and communication channels specify entry, storage, processing and transmission of information. With these process points, the information asset's processing security objectives are evaluated. For each EP, PP and CC, the degree of security functions' implementation (like access control, authorisation, data validation, communication, encryption, performance and measures) are determined. These security functions are to be evaluated, as they are closely linked to security objectives by their definition (see section 2.3 for a definition of the security objectives). To take an example, integrity is about the protection of the accuracy and completeness; therefore access control, authorisations and data validation are verified to ensure integrity. Confidentiality is about the prevention of unauthorised disclosure and therefore access control, authorisation, communication and encryption are verified to ensure confidentiality. Availability means that assets are accessible and therefore implemented contingency measures and system performance are verified to ensure availability. Table 5-3 shows all possible ratings defined for access control (AC), authorisation (A), data input validation (D), communication (C) and encryption (E). For each level, its rating and abbreviation is defined, e.g. AC0 means Access Control Level 0; A2 means Authorisation Level 2. After determining the security function implementation levels, the adherence to the information asset's security objective at each EP, PP and CC, where the information asset is utilised, has to be determined.

Table 5-3: EP, PP and CC rating criteria

EP/PP measures			**CC measures**	
Access control & accountability	Authorisation (access right)	Data input validation	Communication	Encryption
AC0: unauthenticated user	A0: none	D0: None	C0: External unauthenticated partner	E0: None
AC1: internal user	A1: Read	D1: Manual	C1: External authenticated partner	E1: Weak encryption
AC2: authenticated user	A2: Execute/ process	D2: Downstream validation	C2: Internal network partner	E2: Standard encryption
AC3: System user	A3: Write/ update	D3: Value verification	C3: Internal authenticated partner	E3: Strong encryption
	A4: Full control	D4: Value verification and completeness		
EP/PP security level			**CC security level**	
Not applicable (n/a), Unknown (u), insufficient (nok), sufficient/best practice (ok)				

Step 3.1 - Asses processing of information assets (activity two)

In this second activity of step 3.1, the security functions' implementation rating for each EP, PP and CC is evaluated with regard to the security objective level of the information asset. Subject to the process point - an action on information - and the security objective, a set of security functions is evaluated considering the action on information and the security objective to be achieved. EPs are only evaluated with regard to integrity by the security functions access control and data validation. PPs are evaluated based on integrity and confidentiality by the security functions access control, authorisation and data validation. CCs are evaluated with regard to integrity and confidentiality by the security functions' communication and encryption. Availability is rated for EPs, PPs and CCs which use systems by system performance and contingency measures. The evaluation of the security function implementation rating with regard to the security objective rating of the information asset is supported by a predefined set of rules to verify adherence. For

example, the evaluation of access control at EP1 (Entry Point 1) rated as AC0 (Access control level 0) is compared against defined rules for the security objective integrity level 2. Figure 5-2 is an excerpt of the rule set in table form, defined for the security objectives integrity and confidentiality. The complete rule set can be found in appendix A.5. The rating for an EP/PP and CC can be ‘ok’ (sufficient - requirements are adhered to), ‘nok’ (insufficient - requirements are not adhered to), ‘n/a’ (not applicable) or ‘u’ (unknown - no rating possible). The rules can be read as follows for integrity level one and the security function access control (in each cell, one or more rules are presented):

- AC0: If an EP is rated as AC0 then the data input validation rating has to be at least a D2 for that EP. A PP rating of AC0 is ok;
- AC1 and AC2: If an EP is rated as AC1 or AC2 the data input validation rating has to be least D1. A PP rating of AC1/AC2 is ok;
- AC3: An EP rating of AC3 is ok. A PP rating of AC3 is ok.

Security Objective / Security Concept		Integrity Level 1	Level 2	Level 3	Confidentiality Level 1	Level 2	Level 3
Access Control							
unauthenticated user	AC0	EP and >= D2 PP	EP and D4 PP and <= A1	EP failed PP and <= A1	PP and <= A2	PP failed	PP failed
internal user	AC1	EP and >= D1 PP	EP and >= D2 PP and <= A2	EP failed PP and <= A1	PP and <= A3	PP and <= A3	PP failed
authenticated user	AC2	EP and >= D1 PP	EP and >= D1 PP and A3 and >=D1	EP and >= D2 PP and (A3 or A4 and D4)	PP	PP	PP and <= A3
System user	AC3	EP PP	EP PP	EP PP	PP	PP	PP
Authorization							
none	A0	PP	PP	PP	PP	PP failed	PP failed
Read	A1	PP	PP	PP	PP	PP and >= AC1	PP and >= AC2
Execute/process	A2	PP	PP >= AC1	PP and >= AC2	PP	PP and >= AC1	PP and >= AC2
Write/update	A3	PP and >= D3	PP and D4 or AC2 and >= D1	PP and (AC2 and D4) or AC 3	PP and >= AC1	PP and >= AC1	PP and >= AC2
Full control	A4	PP and >= D3	PP and D4 or (AC2 and D2)	PP and (AC2 and D4) or AC 3	PP and >= AC2	PP and >= AC2	PP and >= AC2
Data validation							
None	D0	EP failed	EP failed	EP failed	n/a	n/a	n/a
Manual	D1	EP and >= AC1	EP and AC2	EP failed	n/a	n/a	n/a
downstream resonableness validation	D2	EP	EP and >= AC1	EP and AC2	n/a	n/a	n/a
Value verification	D3	EP	EP and AC2	EP and AC2	n/a	n/a	n/a
Value verification and completeness	D4	EP	EP	EP and AC2	n/a	n/a	n/a
Communication							
External unauthenticated	C0	CC and >= E1	CC failed	CC failed	CC and >=E1	CC and >= E2	CC failed
External authenticated partner	C1	CC	CC and >= E2	CC and E3	CC and >=E1	CC and >= E2	CC and E3
Internal network partner	C2	CC	CC	CC and >= E2	CC	CC	CC and >= E2
Internal authenticated partner	C3	CC	CC	CC	CC	CC	CC
Encryption							
none	E0	CC failed	CC failed	CC failed	CC and >=C2	CC failed	CC failed
weak encryption	E1	CC	CC failed	CC failed	CC	CC failed	CC failed
Standard encryption	E2	CC	CC	CC failed	CC	CC	CC failed
strong encryption	E3	CC	CC	CC	CC	CC	CC

Figure 5-2 Security objective rule set table

The evaluation of the information asset security objective integrity and confidentiality is based on the same security functions and follows the same procedure. For the security objective availability, different categories like “performance” and “measures” are used. It is evaluated how often availability requirements were met in the past with the “performance” rating. Implemented

continuity measures are evaluated with the “measures” rating. The difference to the assessment of integrity and confidentiality is that in the availability assessment only system containers are evaluated. The rule sets are not static and can be adopted if company-specific policies require this. The rules were defined using security expert knowledge and considering security function dependencies with regard to the security objective level. For example, dependencies between access control and authorisation, as well as data validation, with regard to information entry or processing were considered at the rules. The rule set shown in Figure 5-2 was implemented in (SWI-)Prolog (http://www.swi-prolog.org/) to support the assessment (see appendix A.6 for the complete program), which is briefly explained in the following.

Introduction to automated security objective evaluation with Prolog

The objective of the Prolog program (see section A.6) is to support automated assessment of security objectives. In Prolog, the program logic is expressed in facts and rules. The program is begun with a query, which the Prolog engine tries to satisfy by verifying the facts and rules available. The facts and rules represent the security objective rules of Figure 5-2. For each security objective (integrity, confidentiality and availability), a security rating (level 1 to 3) with regard to an EP, PP, CC facts was defined. These facts are verified by Prolog rules, as to whether the query becomes true. For rules of the rule set table representing a condition, a fact is used, for example, a PP is ok (true) when the security function authorisation is rated as A0 - `authorisation(a0).` For rules which represent a conditional statement, a fact with arguments is used, e.g. a PP is ok (true) when the security function authorisation is rated A0, and access AC1 - `authorisation_access(a0,ac1).` In order to represent dependencies

between a condition and a conditional statement, rules for integrity, confidentiality and availability were used. That is to say, both facts above are combined by a logical conjunction (‘and’ represented by a comma) in a rule:

```
integrity(A,Ac):- authorisation(A), authorisation_access(A,Ac).
```

With Prolog rules and logical conjunctions, facts and conditional statements can be combined. These can include or exclude conditions, or form a new condition. Prolog was chosen, because logical specifications of searches can be defined in order to determine when the security function implementation becomes true with regard to the security objective level. This Prolog characteristic can also be used for determining what security functions are needed - if not known - to comply with a security objective level. Furthermore, in Prolog, the rule base can be changed easily, or rules can be enhanced if required (i.e., if additional security functions have to be evaluated or if new facts are available).

The program (see section A.6) consists of three main parts - the facts which represent single conditions for security objectives and process points, the assessment rules for security objectives and process points and the query interface to request the assessment information needed from the user. These three parts are explained briefly in the following:

1. Query interface

The program starts with `assess.` by asking for the security objective (`X` = confidentiality, integrity or availability) and rating (`Lev` = level 1 to 3). Next, the process point type (`Pp` = ep, pp or cc) is asked by the rule `so(X,Lev)`, and dependent of the security objective entry the rule `integrity(Pp, Lev)`, `confidentiality(Pp, Lev)` or `availability(Lev)` called. At `integrity(Pp, Lev)` and `confidentiality(Pp, Lev)` the EPs’ and PPs’

security functions ratings are asked for access control (`Ac` = ac0 to ac3), authorisation (`A` = a1 to a4) and data validation (`D` = d1 to d4). For CCs only the ratings for encryption (`E` = e0 to e3) and communication (`C` = c0 to c3) are asked. At `availability(Lev)` the performance (`P` = p1 to p4) and measures (`M` = m1 to m4) rating of systems of an EP, PP and CC is asked. The input can only be provided for one EP, PP or CC. The input of a security function can be omitted if not available (e.g. by '[]') or asked to be resolved by Prolog using a variable (e.g. 'Result'). After that, depending on which security objective was specified, the corresponding assessment rules for availability, integrity or confidentiality with regard to the process point type are called, as explained below. The program only evaluates one security objective for one process point.

2. Assessment rules

The assessment rules are called after the user specified the security functions for an EP, PP or CC to evaluate the adherence of the security objective.

Integrity is evaluated for EPs, PPs and CCs. The following rules were defined:

```
integrity_PP(Lev,Ac,A,D):-(pp_int_access(Lev,Ac);
pp_int_auth(Lev,A); pp_int_access_auth(Lev,Ac,A,D)).

integrity_EP(Lev,Ac,D):-
(ep_int_data(Lev,D);ep_int_access(Lev,Ac);ep_int_data_access(
Lev,Ac,D)).

integrity_CC(Lev,C,E):-
(cc_int_com(Lev,C);cc_int_enc(Lev,E);cc_int_com_enc(Lev,C,E))
,not(cc_int_com_enc_no(Lev,C,E)).
```

The body of each rule checks whether a single variable or a combination of all the variables is true with regard to the facts defined. For example, for an EP, whether the security function rating Ac or D is true, or Ac *and* D is true. Lev contains the security objective level and is only used to distinguish between the facts defined for the different security objective levels.

Confidentiality is only evaluated at PPs and CCs; for EP, no confidentiality requirements from a processing view have to be adhered to. The following rules were defined:

```
confidentiality_PP(Lev,Ac,A):-
(pp_conf_access(Lev,Ac);pp_conf_auth(Lev,A);pp_conf_access_auth(Lev,Ac,A)).

confidentiality_CC(Lev,C,E):-
(cc_conf_com(Lev,C);cc_conf_enc(Lev,E);cc_conf_com_enc(Lev,C,E)),not(cc_conf_com_enc_no(Lev,C,E)).
```

The body of each rule is checking whether a single variable or a combination of all the variables is true with regard to the facts defined. For a PP, whether the security function rating Ac or A is true or Ac and A is true. Lev contains the security objective level and is only used to distinguish between the facts defined for the different security objective levels.

Availability is evaluated without a distinction between EPs, PPs and CCs and therefore directly by the facts defined. The rule `availability_EPPPCC(Lev,P,M).` verifies the ratings for performance and measure using the facts defined for an availability level. Lev contains the security objective level and is only used to distinguish between the facts defined for the different security objective levels.

3. Facts

The facts defined describe a true condition for an EP, PP and CC for integrity, confidentiality and availability with regard to the security function implementation. The facts are used by the assessment rules to verify whether the statement for an EP, PP or CC is true. The facts were constructed as follows:

```
Name_of_the_fact(Security objective level, security function rating).
```

The security function rating of the rule can be one or more arguments.

Step 3.2 - Assess container of information assets

At step 3.2, the information assets' containers (e.g. systems, actors, environment) are evaluated with regard to information assets' security requirements. The textual security requirements of information assets' containers are evaluated at each process activity where information processing takes place, in the form of EP, PP and CC, using information-gathering techniques such as on-site interviews and document reviews. The identified EP, PP and CC are assessed by the security expert, based on the evidence for whether the security requirement for the system, organisation or physical environment is adhered to (this evidence can be gathered from the system configuration, the system specification, the company's security policy, process documentation or examples of implementation). IT security processes are evaluated by system testing, documentation reviews and process performance documentation reviews. The IT security process evaluation supports identifying technical issues and secure operation; it also determines the organisation's capability to detect, prevent or mitigate security issues. IT process security is indicated by whether issues are identified in the process or not.

5.2.4. Phase 4 – Risk documentation

Phase 4 of the approach is about risk result documentation. The overall assessment result (for security objectives and requirements) of an information asset concerning all EP, PP and CC ratings for processing and containers in the process is determined by consolidating the results. This means all EP(1-x), PP(1-x) or CC(1-x) associated to an information asset in a process are checked for whether the processing or containers' results indicate adherence or non-adherence. If there is any failure (nok) then the processing or containers will be rated as 'nok' for the information asset. Then, the issue causing this non-

adherence is identified and documented in the risk result documentation for the process and information asset.

At the end of the assessment, all information assets at risk are presented (see Table 5-4). The results table shows the business processes, the issue associated (with an ‘X’), as well as the affected information asset. The risk result indicates - using ‘not at risk’ or ‘at risk’ - whether an information asset is vulnerable in a business or IT process, because the requirements for processing or containers of an information asset were not adhered to, or because IT processes do not perform properly. Probabilities don’t have to be specified, because the non-compliance causing harm to the organisation is determined. Basically, deviations in operation and implementation from the security needed (specified as security objectives and requirements) are identified, represented as a vulnerability, and defined as risk. Furthermore, the result can also indicate the absence of security risk, as the security requirements - business security needs - were evaluated in the business context regarding security functions.

Table 5-4: Risk result documentation

Processes/Issues - Information asset	**Information asset**	**Information asset**
Business Process name	**at risk**	**at risk**
Issue		
Issue	X	X
Issue	X	

5.3. Running example

In the following, a real world example, modelled in Business Process Modelling Notation (BPMN), is used to demonstrate the applicability of the approach in a practical and realistic environment.

5.3.1. Process Modelling Notation (BPMN)

The example process is modelled in Business Process Modelling Notation (BPMN) (OMG, 2009) (see Figure 5-3), a quite new proposal in comparison to existing process modelling notations like ARIS (IDS Scheer, 1994), whose notation considers a unique diagram for the representation of business processes. According to the state of the business process modelling industry, BPMN is among the most commonly used standards for process modelling. It was designed to facilitate use and understanding, as well as to bridge the gap between business process modelling and business process implementation (OMG, 2009). In this thesis, BPMN was used because it is open - the standard is directly available - and extensible - elements can be added. For example, Rodriguez et al. (2007) defined a BPMN extension to model security requirements within a business process diagram that can be attached to any business process model elements. However, in this thesis, only BPMN standard objects like data object, association and text annotation were used for presenting evaluation results; no extension for the evaluation or result documentation was defined. The reason for this is that the objective was to use BPMN standard model elements as extensions are not self-explanatory, and might be lost during the interchange of models (OMG, 2009). In addition, it was not the aim of this thesis to model security risk assessment information or to perform any automatic processing or evaluation of the model. Furthermore, with the process example modelled in BPMN, also the applicability of our assessment approach - the evaluation and documentation of results - using standard BPMN models is demonstrated.

5.3.2. BPMN process example

Process model - online travel insurance quotation: A major part of the turnover of an insurance company is created via an online system offering travel insurance. The travel insurance for vacations, business trips and other time abroad, is concluded when the customer has provided all data (name, address, email, phone number, date of birth, travel details) and agreed to the terms and conditions of the company. Payments can be made via credit card or debit payment and the insurance contract is then sent per email and post. The online system is a web application with a connected database storing all data about the contract. It also has an interface to a third-party service to verify credit card and bank account data, as well as to the accounting system for payment processing. As this is an example for illustration purposes, we know already (before applying the approach) that the online system has a code injection problem when personal data is entered (at process activity 3 - ‘Display product details ...’), and an encryption problem at the interface with the third-party service (at process activity 4 - ‘Verify personal and payment data’). In addition, the information technology (IT) continuity management process is not documented and tested. The BPMN model of the process is as follows:

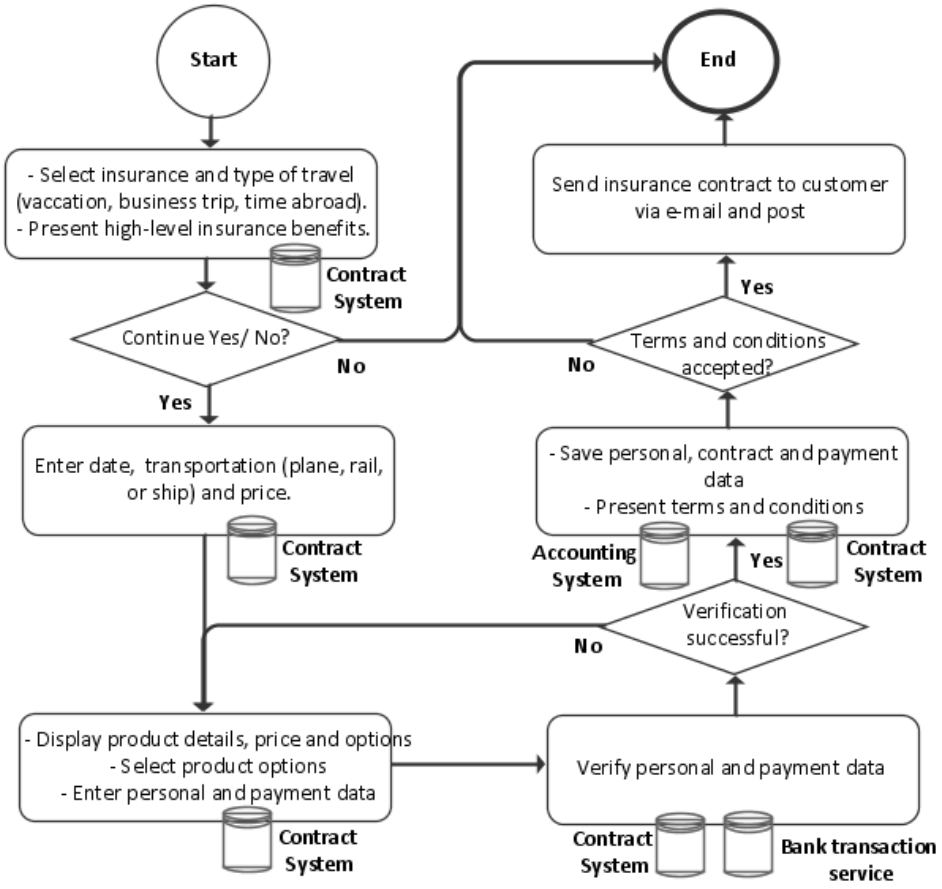


Figure 5-3 BPMN process model online insurance quotation

5.3.3. Phase 1 - Asset identification

Step 1.1 of the approach - identify critical business processes - is omitted, as in this example only one critical business process (the online insurance quotation process) is available. In step 1.2, the following information assets were identified in the online insurance quotation process: customer and payment data. Customer data is saved and processed, as along with payment data needed for the transactions. Criteria and indicators for identifying these information assets are decision points and activities in the process like ‘Enter personal and payment data’, ‘Verify personnel and payment data’, or ‘Save personnel, contract and payment data’.

5.3.4. Phase 2 - Asset profiling

In this phase, the information asset's security requirements have to be specified. Firstly, the appropriate security objective rating for integrity, confidentiality and availability should be selected based on the security needs of the information asset. Secondly, the container security requirements should be specified; describing what is to be protected as well as the concrete implementation at the containers handling the information. To elicit and define the security requirements, one can use the company's security policy, organisational procedures and security best practices. For the definition of IT security processes which ensure and operationalise security, IT operations guidelines like ITIL (CCTA, 2007), or security standards can be used. Table 5-5 and Table 5-6 show the security requirements defined for customer and payment data.

Table 5-5: Customer data security requirements

Information asset: Customer data		**Integrity**	**Confidentiality**	**Availability**	**IT Security Processes**
Processing	Data	I-L2	C-L2	A-L3	n/a
Containers	Primary Systems	Address data has to be verified in the system. Data in the system should be protected against unauthorised access and modification. 192-bit AES encryption if data is transferred.	Access should be given only to company people. Changes have to be logged.	Within one business day.	Access Management (authorisations) IT Security Management (Security of systems) Continuity management and Disaster Recovery Change Management
	Organisation People Process	Personnel entering data should verify their entries as well as the data received.	People of the departments should be aware of confidentiality.	Core people within one business day.	Access Management IT Security training
	Physical	None.	Documents should be locked away and disposed of securely.	Within one business day.	IT Security training Facility Management Continuity Management

Table 5-6: Payment data security requirements

Information asset: Payment data		Integrity	Confidentiality	Availability	IT Security Processes
Processing	Data	I-L2	C-L2	A-L2	n/a
Containers	Primary Systems	Data in the system should be protected against unauthorised access and modification. 192-bit AES encryption if data is transferred.	Access should be given only to company people. Changes have to be logged.	Within two business days.	Access Management (authorisations) IT Security Management (Security of systems) Continuity management and Disaster Recovery Change Management
	Organisation People Process	Personnel entering data should verify payment data details. Payment data details should be externally verified.	People of the departments should be aware of confidentiality.	Core people within two business days.	Access Management IT Security training
	Physical	None	Documents should be locked away and disposed of securely.	Within two business days.	IT Security training Facility Management Continuity Management

5.3.5. Phase 3 - Vulnerability identification

Firstly, at step 3.1 of the approach, the degree of implemented security functions in information processing and their adherence to information assets' security objectives are evaluated. Secondly at step 3.2, the information assets' containers (systems, actors, and environment) are evaluated based on information assets' security requirements.

Step 3.1 - Assess processing of information assets

The first step is to determine where the information assets in the process are created, processed or transmitted. The EP, PP and CC were identified by keywords (e.g. enter, save, send) of process activities' descriptions. In the BPMN online insurance quotation process, the numbered EP, PP and CC points represent these identified processing points (see Figure 5-4). Furthermore, each

EP, PP and CC is associated with the information assets that are processed at these points (see Figure 5-5). Secondly, for each EP, PP and CC, the degree of security function implementation (including access control, authorisation, data validation and communication security) is determined. Then, the adherence to the information assets security objective at each EP, PP and CC is determined by the rule set. In Table 5-7, the columns ‘Entry, Process and Communication points rating’, ‘Processing (SO) Assessment’ and ‘Processing result’ show the security function ratings, the security objective assessment results and the overall assessment results for an EP, PP or CC at this step. For determining the ‘Processing (SO) Assessment’ results in the table, the Prolog program of section A.6 can be used, with the input of the ‘Entry, Process and Communication points rating’.

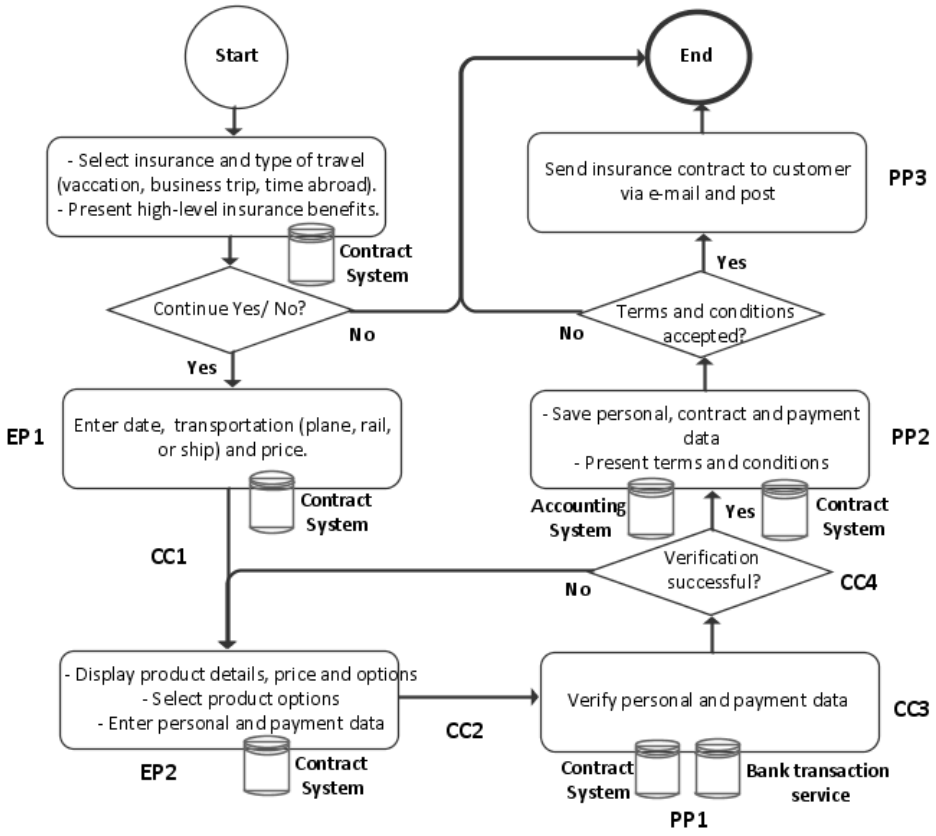


Figure 5-4 BPMN online insurance quotation with identified EP, PP and CC

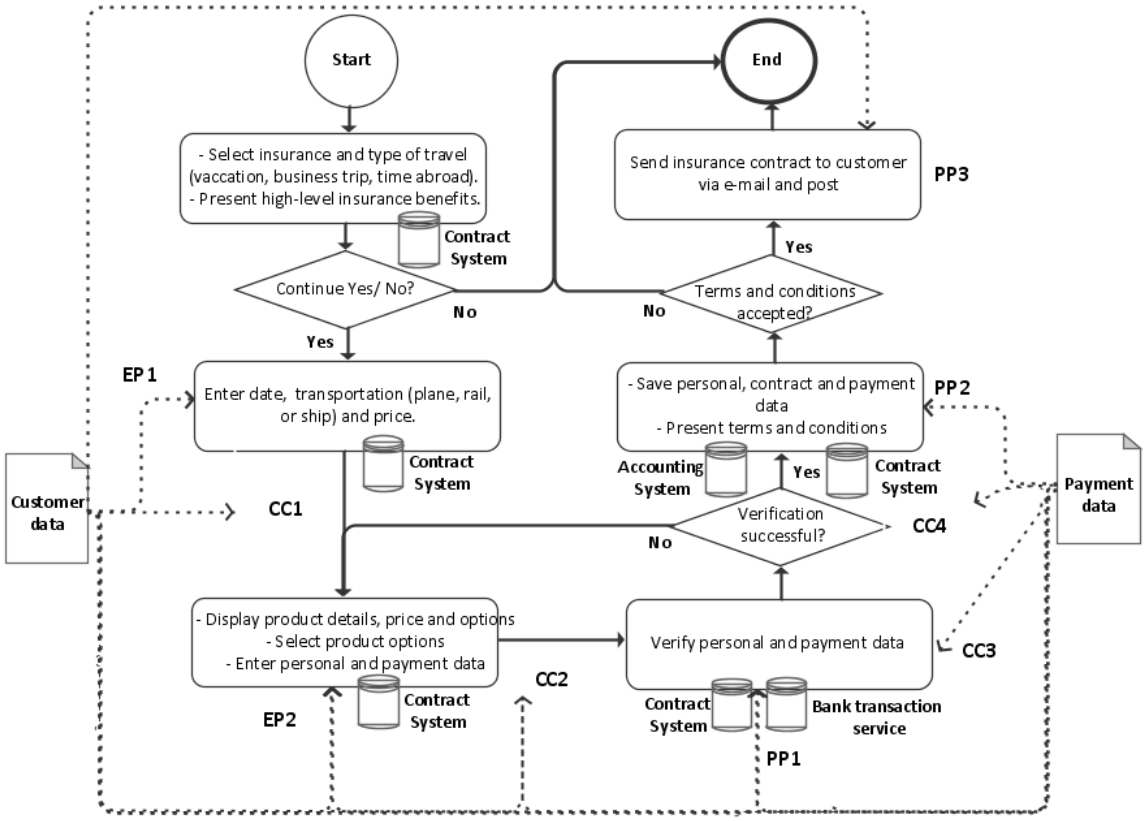


Figure 5-5 BPMN online insurance quotation with EP, PP, CC and information assets

Step 3.2 - Assess containers of information assets

The containers' security requirements are evaluated by the security expert at each process activity where data processing (EP, PP, CC points) takes place. The evidence for whether the security requirement for the system (PiSys), organisation (Org) or physical environment (Phy) is adhered to can be gathered from the system configuration or specification, the company's security policy, process documentation or other examples of implementation. This means that, for each container of the information asset, the assessor has to evaluate the security requirement with the current system implementation and examine the environment of the actor and system where the information is processed.

Table 5-7 ‘Container (SR) Assessment’ shows the results of the containers’ security requirements (SR) at each EP, PP, CC.

Table 5-7 Evaluation results for EP, PP and CC

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): Cust. data	AC0	A0	D4	ok		ok	ok	ok	na	na
EP(2): Cust. data	AC0	A0	D4	ok		ok	ok	nok	na	na
EP(2): Pay. data	AC0	A0	D4	ok		ok	ok	ok	na	na
PP	**AC**	**A**	**D**	**I**	**C**	**A**	**PP**	**PiSys**	**Org**	**Phy**
PP(1): Cust. data	AC3	A3	D3	ok	ok	ok	ok	nok	ok	ok
PP(1): Pay. data	AC3	A3	D3	ok	ok	ok	ok	nok	ok	ok
PP(2): Cust. data	AC3	A3	D1	ok	ok	ok	ok	ok	na	ok
PP(2): Pay. data	AC3	A3	D1	ok	ok	ok	ok	ok	na	ok
PP(3): Cust. data	AC3	A3	D0	ok	ok	ok	ok	ok	ok	ok
CC	**C**	**E**		**I**	**C**	**A**	**CC**	**PiSys**	**Org**	**Phy**
CC(1): Cust. data	C0	E2		nok	nok	ok	ok	ok	na	na
CC(2): Cust. data	C1	E2		ok	ok	ok	ok	ok	na	na
CC(2): Pay. data	C1	E2		ok	ok	ok	ok	ok	na	na
CC(3): Cust. data	C1	E1		nok	nok	ok	nok	nok	na	na
CC(3): Pay. data	C1	E1		nok	nok	ok	nok	nok	na	na
CC(4): Cust. data	C1	E2		ok	ok	ok	ok	ok	na	na
CC(4): Pay. data	C1	E2		ok	ok	ok	ok	ok	na	na

Result Explanation: EP2 was rated ok for processing however nok for the container (PiSys), because it was possible to change data of the system via code injection at customer data entry fields. PP1 was rated as ok for processing but nok for the container (PiSys), because of the missing encryption for both customer and payment data - which is required. CC1 was rated nok for processing, however the result manually set to ok, as a new customer cannot be authenticated. CC3 was rated nok for the processing as well as the container (PiSys) for both data forms, because of the weak encryption between the company and the bank transaction service. At least a standard encryption service should be implemented.

Processing and Container evaluation results in the process model

Figure 5-6 shows the BPMN (OMG, 2009) online travel insurance quotation process with the evaluation results for processing, as well as for containers' security requirements. At each activity where data processing takes place, the EPs and PPs processing and containers are rated. CCs are evaluated between activities and decisions. The BPMN data object and BPMN associations are used to indicate where the BPMN data object is used in the process and where an evaluation was performed. Therefore, the BPMN data object - defined once in the process - was aligned using associations to process activities or decisions of the process where EP, PP or CC were identified. Identified EP, PP and CC points were presented with a BPMN textual annotation containing all consolidated evaluation results of each point. The BPMN data object was also used to present the consolidated results of all EP, PP and CC for the information asset. The property attribute of the BPMN data object could be used to contain the business security requirements - the data, primary system, actor/organisation, as well as physical requirements - but this was not used. The IT security process evaluation results are not documented in the BPMN process model; they are only documented at phase 4.

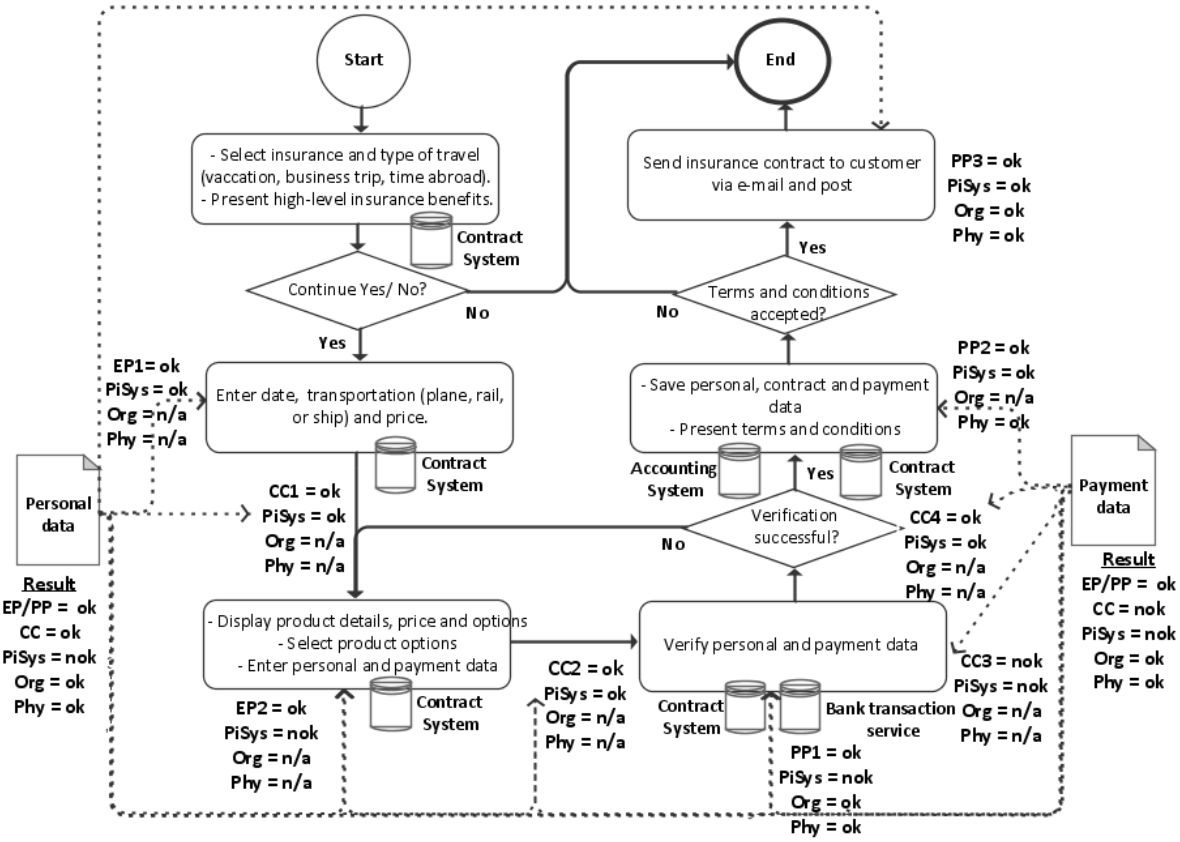


Figure 5-6 BPMN order process with evaluation information

Evaluation of IT security processes of information assets

The IT security processes of the security requirements specification are evaluated by system testing and process performance documentation reviews of the assessor. For the specified IT security processes, the assessor has to determine how mature the processes are, as well as whether they are periodically and accurately performed. The detailed requirements in the field of IT security processes can be reused from IT operation guidelines like ITIL (CCTA, 2007), or security objective standards like COBIT (ITGI, 2007). In our example, the IT security processes Access Management, IT Security Management, Change Management, Continuity Management and Disaster Recovery, IT Security Training and Facility Management were evaluated based on the ITIL process structure. Table 5-8 shows a list of ITIL processes and the results.

Table 5-8: IT security process assessment results

IT process name	Sub-process name or Control Objective	Evaluated	Affected Data	Identified issue
Service Strategy	Service Portfolio Management	no		
	Financial Management	no		
Service Design	Service Catalogue Management	no		
	Service Level Management	no		
	Risk Management	no		
	Capacity Management	no		
	Availability Management	no		
	IT Service Continuity Management	yes	all	Documentation was not up-to-date and not all applications were tested.
	IT Security Management	yes	all	No issues identified.
	Compliance Management	no		
	IT Architecture Management	no		
	Supplier Management	no		
Service Transition	Change Management	yes	all	No issues identified.
	Project Management	no		
	Release and Deployment Management	no		
	Service Validation and Test	no		
	Application Development and Test	no		
	Service Asset and Configuration Management	no		
	Knowledge Management	no		
Service Operation	Event Management	no		
	Incident Management	no		
	Request Fulfilment	no		
	Access Management	yes	all	No issues identified.
	Problem Management	no		
	IT Operations Management	yes	all	No issues identified.
	IT Facilities Management	yes	all	No issues identified.
Continual Service Improvement	Service Evaluation	no		
	Process evaluation	no		
	Definition of process improvements	no		
	Tracking of improvements	no		

In our example, the IT Service Continuity Management, the IT Security Management, the Change Management, the Access Management, the IT Operations Management and the IT Facilities Management processes were evaluated. For each process, whether it was evaluated and whether all information

assets would be affected are both indicated. The processes were evaluated with regard to the following objectives:

IT Service Continuity Management: Continuity measures for applications were evaluated, along with whether disaster recovery and business continuity processes were documented and regularly tested.

IT Security Management: Whether someone is responsible for security management was checked, and whether processes and policies are in place to ensure the security of information. Especially, the presence of security guidelines for systems and a security policy for employees was established, and whether systems are evaluated for appropriateness of controls and associated risks was tested.

Change Management: The change management process for applications in place was evaluated. Especially, the change management for the online web store was evaluated and how the process was performed during the last changes made to the system.

Access Management: The access management process was evaluated; especially in terms of how access is granted/revoked for applications.

IT Operations Management: The operation of systems was evaluated, based on whether process are in place for the maintenance of systems, whether systems operation is monitored and the automatic/manual job scheduling.

IT Facilities Management: The facilities for the systems were evaluated for whether fire detection and prevention systems are installed and maintained, and whether information can be locked away at workplaces.

5.3.6. Phase 4 – Risk documentation

At the end of the assessment, the information asset at risk within the business processes and the issue (with an ‘X’) is presented (see Table 5-9). The result indicates - by ‘not at risk’ or ‘at risk’ - whether an information asset is vulnerable in a business process. In the online travel insurance quotation process, customer and payment data is vulnerable because of the code injection and encryption issues. Furthermore, the issue of the IT continuity management process causes the information assets to be at risk. The overall results of the business process evaluation and the IT security process evaluation contain only vulnerabilities and risks associated for that process. If no vulnerabilities and risks were identified, then the online travel insurance quotation process would be ‘not at risk’ and information defined as secure.

Table 5-9: Overall result documentation

Processes/Issues - Information asset	**Customer data**	**Payment data**
Online travel insurance quotation process	**at risk**	**at risk**
Contract system - injection/ unauthorised access	X	X
Bank transaction service - weak encryption	X	X
IT service continuity management	X	X

5.4. Chapter summary

In this chapter, the details of the security requirements risk assessment approach were presented and the procedure explained theoretically, as well as with a running example from the insurance sector. The evaluation of vulnerabilities and risks is based on the information assets’ processing and containers handling the information in business process models. Security objectives are specified for the processing of information, and security requirements for the containers handling information assets which are evaluated. Both are evaluated at entry-, process- and

communication points in the business process model, where information in the process is entered, processed or communicated respectively. Security objectives are evaluated for their implemented security functions based on a rule set. Security requirements are evaluated for the containers - systems, actors and the environment - whether they are adhered to within the business process context. Furthermore, IT security processes defined in the information assets' security requirements specification are evaluated as to whether they prevent or detect vulnerabilities, and ensure the secure operation of systems to determine any IT operation or technical vulnerabilities. At the end of the evaluation, identified vulnerabilities (namely risks affecting information assets at processes) are documented; they could cause harm the organisation, and thus represent a risk.

Chapter 6 - Validation

In this chapter, the validation of the security requirement risk assessment approach is performed using three validation criteria: the *methods procedure,* defining and using security requirements systematically; the proposed approach's *result accuracy* regarding a best practice approach; and the *methods capability* to resolve vulnerability identification errors.

6.1. Validation criteria

The security requirements risk assessment procedure is validated by three validation criteria by different methods, in order not to rely just on one validation result and in order to be able to make independent statements about using security requirements for vulnerability identification if one fails. The criteria are briefly explained in the following, and in the corresponding sections of this chapter, the validation execution, results, interpretation, and threats to validity are discussed for each criterion.

(1) Methods procedure

With this criterion, it is illustrated that an asset's security requirements are evaluated systematically at the proposed approach for identifying vulnerabilities. Validation is performed by assertion and document analysis of current approaches and procedures, as to how security requirements are defined and used for vulnerability identification. In addition, a proof of concept is conducted implementing the proposed approach as a pseudo-code program, to demonstrate that the approach's procedure can be formally defined.

(2) Result accuracy

With this criterion, the accuracy of the proposed security requirements risk assessment approach in determining (positive) vulnerabilities is verified. In particular, it is tested whether vulnerabilities are identified at least as accurately as with an alternative best practice risk assessment approach. Validation of this criterion is performed through testing, applying both approaches at three entities of a global insurance company at the same time.

(3) Method capability

With this criterion, it is demonstrated that using business process models and security requirements can resolve vulnerability identification errors (false positives), as well as that vulnerability identification errors do occur. Validation of this criterion is performed by a quasi-experiment using a survey of security professionals.

6.2. Methods procedure

In this section, it is illustrated that security requirements are evaluated systematically at the security requirements risk assessment approach for identifying vulnerabilities. Therefore, it is compared how security requirements are firstly *defined,* and secondly *used,* for vulnerability identification within current approaches like Octave Allegro (Caralli et al., 2007), NIST SP 800-30 (Stoneburner et al., 2002b) and Innerhofer-Oberperfler and Breu (Breu and Innerhofer-Oberperfler, 2005). Furthermore, it is demonstrated that the proposed approach can be formally defined by a pseudo-code program.

6.2.1. Analysis of security requirements utilization

In the literature review of chapter 3, three information security risk assessment approaches were identified, which use security requirements and are closely

related to the proposed approach: OCTAVE Allegro (Caralli et al., 2007), NIST SP 800-30 (Stoneburner et al., 2002b) and Innerhofer–Oberperfler and Breu (2006). In the following, the phases and activities of these approaches are compared, where security requirements (SR) are *defined* and *used* in the assessment for vulnerability identification, and in order to examine the systematic utilisation of security requirements for vulnerability identification. Figure 6-1 shows the phases and activities identified where security requirements are defined and used in each approach. The headings above the rectangles name the phases, and the rectangles describe the activity alongside the step number in the approach. The grey area in the figure highlights the activities where security requirements are *defined,* and the blank area where security requirements are *used* in each approach.

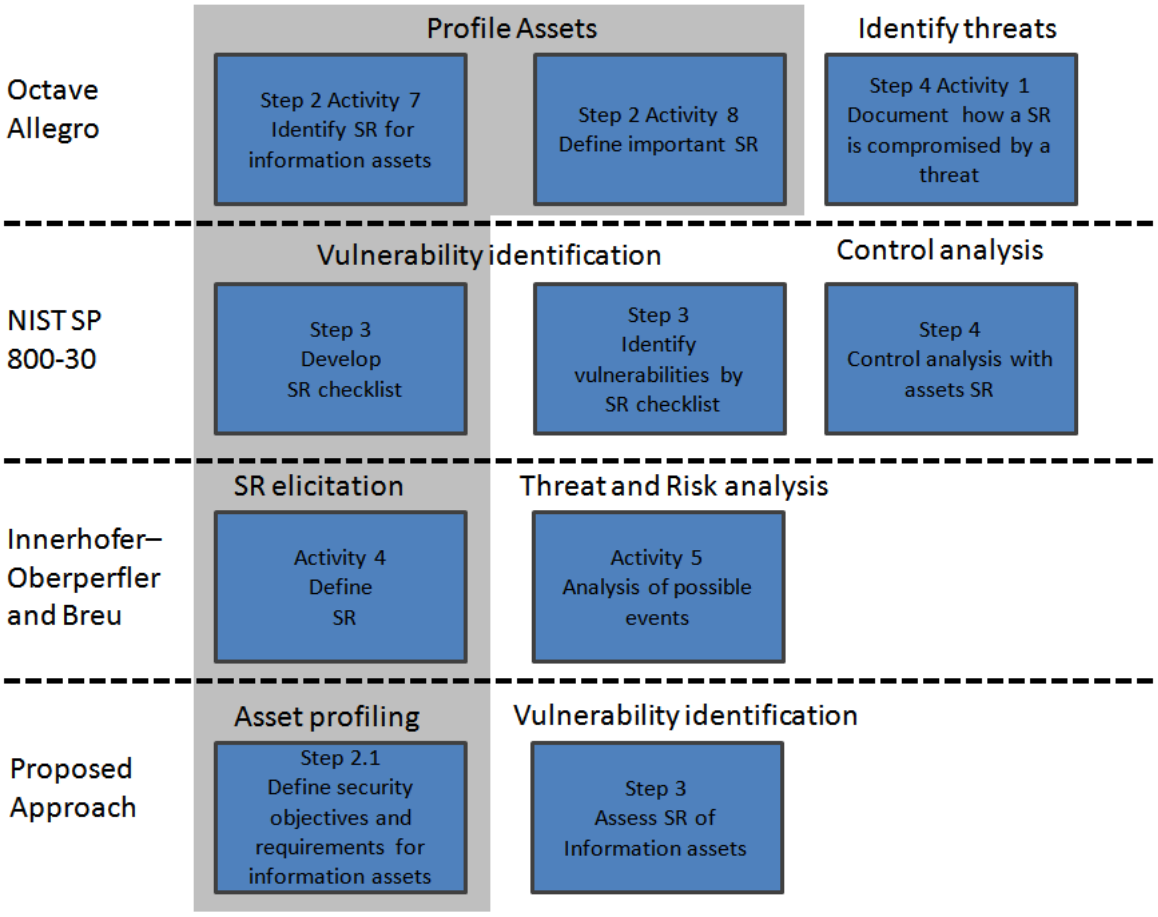


Figure 6-1 Comparison of security requirement usage in the assessment approaches

Below, it is illustrated in detail how security requirements are *defined* and *used* in the risk assessment of all these approaches. In OCTAVE Allegro (Caralli et al., 2007) at step 2 activity 7, security requirements for confidentiality, integrity and availability are defined for critical information assets identified. At step 2 activity 8, the most important security requirement has to be chosen for use later in order to determine the potential impact of a risk. Step 4 activity 1 in OCTAVE Allegro is about threat identification. Threats are identified for assets by brainstorming; the assessor has to "keep in mind the security requirements that you have set for your information asset and how they might be compromised due to a threat" (Caralli et al., 2007, p. 46). In step 4 activity 1, the assessor has to document how the threat would compromise the security requirement. Then, later in the assessment, the risk is determined by the consequence and the severity of the threat based on risk criteria established at the beginning of the assessment. The security requirement is used as an indicator for the outcome of a threat.

In step 3 of NIST SP 800-30 (Stoneburner et al., 2002b), risk reports, security test results, audit comments and security requirements are used as inputs for vulnerability identification. The recommended methods for identifying vulnerabilities are vulnerability sources, security testing and a security requirements checklist, which "contains the basic security standards that can be used to systematically evaluate and identify the vulnerabilities of the assets" (Stoneburner et al., 2002b, p. 16). "Such a checklist, when created, should contain basic security standards that can be used to evaluate and identify information security vulnerabilities" (West and Andrews, 2004, p.14), as reported in a comparative analysis between NIST and OCTAVE. These basic security standards can come from different areas - like management, operational and technical security - or out of regulatory and security directives, and can include

assignment of responsibilities, data media access and disposal or identification and authentication, representing high level security principles or security control objectives that should be in place and are applied to IT systems.

Innerhofer–Oberperfler and Breu (2006) assign the defined security requirements of step 4 to model elements of their enterprise architecture. Threats have to be identified through existing security checklists or standards like the baseline protection manual (BSI, 2008) or EBIOS (ANSSI, 2010a). At activity 5, an analysis of possible events that can violate the security requirements is performed to determine risk. Threats are assigned to model elements and related to the security requirements. The relation between the model element, threat and security requirement is then used to determine the impact of the threat.

In the proposed approach in this thesis, security requirements are defined for information assets used in business processes (step 2.1). Information assets security requirements are evaluated at process activities where the information is processed, as to whether security functions adhere to the requirements (step 3). Information assets' security requirement dependencies are considered by evaluating the information asset in multiple business processes, and the security control implementation for containers such as systems, actors and the environment.

Differences in defining and using security requirements of the approaches

In all three approaches, security requirements are defined for assets, however the level of detail of *defining security requirements* for assets and *using them for identifying vulnerabilities* is different. Current approaches lack a coherent definition AND usage of security requirements for vulnerability identification; this is summarised in the following:

(a) Definition of security requirements: In NIST SP 800-30 (Stoneburner et al., 2002b), security control objectives are defined applicable for all IT systems representing basic security standards *without any detailed specification* of what should be achieved specific for the asset. Innerhofer–Oberperfler and Breu (2006) define security requirements *generally* for model elements (e.g. a process or system) dependent on the context. This is typed as a textual annotation. In OCTAVE Allegro (Caralli et al., 2007), security requirements are defined for an information asset for confidentiality, availability and integrity, describing what should be achieved. In the proposed approach in this work, security requirements are described based on confidentiality, availability and integrity for an information asset's processing, and for the containers handling the asset at a business process.

(b) Vulnerability identification using security requirements: For the threat or vulnerability identification, OCTAVE Allegro (Caralli et al., 2007) and Innerhofer–Oberperfler and Breu (2006) use security requirements to determine the *impact* of an identified threat and vulnerability. Threats and vulnerabilities are determined by other methods like security checklists, security best practices and brainstorming for an asset or threat scenario. Dependencies are considered by Innerhofer–Oberperfler and Breu (2006) via the model element relations of their enterprise architecture, which consists of process activities and IT systems. These are not considered by the other approaches. In NIST SP 800-30 (Stoneburner et al., 2002b), the security requirements checklist applied to IT systems is used as one method alongside security testing and security vulnerabilities lists *to identify vulnerabilities*. However, the security requirements checklist *lacks of details for the*

security needs of a specific asset, as only basic security standards are evaluated. In the proposed approach, information asset security requirements are evaluated for the processing of information, and for containers handling the information in the business process, to identify vulnerabilities and risks. *Dependencies* are considered via the definition and evaluation of information assets' security requirements at business processes.

Table 6-1 compares how security requirements (SR) are *defined* and *used* for vulnerability identification in these approaches:

Table 6-1: Usage of security requirements

	OCTAVE Allegro (Caralli et al., 2007)	NIST SP 800-30 (Stoneburner et al., 2002b)	Innerhofer–Oberperfler and Breu (2006)	Proposed SR approach
Specific SR definition	Yes	No	Yes	Yes
SR only for assets	Yes	Yes	No	Yes
SR used for impact determination	Yes	No	Yes	Yes
SR used for threat/ vulnerability identification	No	Yes	No	Yes
SR evaluation for a specific asset	No	No	No	Yes
SR dependencies considered	No	No	Yes	Yes

The comparison of the usage of security requirements in Table 6-1 shows that security requirements for assets are only used in the proposed approach and NIST SP 800-30 for vulnerability identification. However, only in the proposed approach are SR used for vulnerability identification AND evaluated specifically for an asset. A reason for this is that, in NIST SP 800-30, security requirements are not asset-specifically defined. Furthermore, in NIST SP 800-30, security requirements' dependencies are not considered in comparison to the proposed SR approach. Therefore, the SR approach is proposed to use security requirements more

systematically for vulnerability identification, as security requirements are specified and evaluated for single assets at business process activities; they can thus consider dependencies.

6.2.2. Proof of concept – The approach in pseudo-code

In this section the security requirements risk assessment approach of section 5.2 is implemented in pseudo-code to demonstrate that the approach is structured and can be implemented as a program. The running example of section 5.3.2 and the UML model of the appendix A.2 – the approach's activities modelled by an UML activity diagram - are used to explain the program code. The input of the program is business process models and as a result, the business process, information asset and vulnerabilities are displayed. In the following, the program is presented using a Pascal programming language-like notation. Brief descriptions with references to the UML model and the running example are included in the program code denoted by [UML] and [Example] respectively, to illustrate the program procedure and processed information.

program Risk identification

/ [UML] Definition of the business process model object*/*

OnlineTravelInsuranceQuotation type of business process;
type business process := record
name, ITprocesses:string,
activity: record;
type activity := record
description, actor, system, environment, informationAsset, ProcessPointTyp, security_functions: string;

/ [UML] Definition of the information asset object*/*

Business Process information assets type of information asset;
type information_asset := record
name, security_objective_level, container_security_requirements, ITprocesses: string;

/ [UML] Definition of the vulnerability object */*

Vulnerabilities type of result;
type result := record
business_process, information_asset, vulnerability: string;

Phase 1 - Asset identification

/ [UML] This procedure represents the partition 'Phase 1 Asset identification' identifying the information assets in the business process. As there is only one BPM, this is the critical BPM. [Example] Input is the Online Travel Insurance Quotation business process.*/*

procedure phase 1 asset identification;
While OnlineTravelInsuranceQuotation.activity **do**
activity.description:= determine informationAsset in activity description;
If an informationAsset is identified **then**
activity.informationAsset:= new information_asset
While information_asset.name **do**
If information_asset.name = new information_asset **then**
Information_asset already defined;
Next information_asset.name
If information_asset not already defined **then**
Information_asset.name:= new information_asset
Next OnlineTravelInsuranceQuotation.activity

/ [Example] Output is the information asset object containing the customer and payment data */*

Phase 2 - Asset profiling

/* [UML] *This procedure represents the partition 'Phase 2 Asset profiling', defining the information assets security objective and requirements. Objects like security best practices and security needs which are used for requirements' definition are not implemented as program code. [Example] Input is the information assets customer and payment data. */*

procedure phase 2 asset profiling;
While information_asset.name **do**
Information_asset.security_objective_level:= set security objective level;
Information_asset.container_security_requirements:= set containers security requirements for PiSys, Phy and Actor;
Information_asset.ITprocesses:= set IT process requirements;
Next information asset.name

/* [*Example] Output is the information asset object containing the customer and payment data now with defined security objectives, container requirements and IT process*/*

Phase 3 - Vulnerability identification

/ [UML] This procedure represents the partition 'Phase 3 Vulnerability identification' identifying EP, PP or CC for each process activity and then specifying the implemented security concepts. Afterwards, the processing and containers' security requirements are evaluated, and at the end the IT processes are evaluated. [Example] Input is the Online Travel Insurance Quotation process and the information assets customer and payment data security requirements.*/*

procedure phase 3 vulnerability identification;
While OnlineTravelInsuranceQuotation.activity **do**

I* [UML] EP, PP, CC and their security functions are identified */*

activity.description:= Determine EP or PP or CC in activity description;
If an EP, PP or CC is identified **then**
activity.ProcessPointTyp:**=** Set typ to 'EP' or 'PP' or 'CC';
activity.security_functions:= Determine implemented security concepts;

/ [UML] EPs, PPs or CCs are evaluated regarding the information assets' security objectives and requirements */*

While Information_asset.name **do**
If activity.informationAsset = information_asset.name **then**
New information_asset:= no;
If activity.security_functions <> information_asset.security_objective_level **then**
Result.business_process:= OnlineTravelInsuranceQuotation.name;
Result.information_asset:= information_asset.name;
Result.vulnerability:= activity.security_functions <> information asset.security_objective_level;
If activity.system <> information_asset.container_security requirements(PiSys) **then**
Result.business_process:= OnlineTravelInsuranceQuotation.name;
Result.information_asset:= information_asset.name;
Result.vulnerability:= activity.system <> information_asset.container_security_requirements(PiSys);
If activity.actor <> information_asset.container_ security_requirements(Org) **then**
Result.business_process:= OnlineTravelInsuranceQuotation.name;
Result.information_asset:= information_asset.name;

Result.vulnerability:= activity.actor <> information_asset.container_security_requirements(actor);
If activity.environment <> information_asset.container_security_requirements(Phy) **then**
Result.business_process:= OnlineTravelInsuranceQuotation.name;
Result.information_asset:= Information_asset.name;
Result.vulnerability:= activity.environment <> information_asset.container_security requirements(Phy);

/ [Example] Output are the identified vulnerabilities - the contract system and the bank transaction service vulnerability - affecting customer and payment data. */*
/ [UML] If a new information asset was identified, phase 1 would be restarted.*/*

If New information_asset = No **then**
Else procedure phase 1 asset identification;

/ [UML] The BPM IT processes are evaluated with regard to the information assets' IT processes */*

OnlineTravelInsuranceQuotation.ITprocesses:= determine implemented IT processes;
While information_asset.name **do**
If OnlineTravelInsuranceQuotation.ITprocesses <> information_asset.ITprocesses **then**
Result.business_process:= OnlineTravelInsuranceQuotation.name;
Result.information_asset:= information_asset.name;
Result.vulnerability:= OnlineTravelInsuranceQuotation. ITprocesses <> information_asset.ITprocesses;

/ [Example] Output is the IT processes' vulnerabilities - the IT service continuity management issue with regard to customer and payment data IT process requirements.*/*

Phase 4 – Risk documentation

/ [UML] This procedure represents the partition 'Phase 4 document risk' presenting the identified vulnerabilities in the business process*/*

procedure phase 4 risk documentation;
While result.business_process **do**
Writeln('Business process name: ', result.business_process);
Write('Vulnerability: ', result.vulnerability;
Write('Affected information asset: ', result.information_asset;

/ [Example] Output are the vulnerabilities for the Online Travel Insurance Quotation process, the contract system and the bank transaction service issue, as well as the IT service continuity management vulnerability affecting customer and payment data. */*

6.2.3. Result interpretation and threats to validity

The pseudo program code demonstrates that the proposed approach can be implemented in a structured program. However, it should be noted that the security objective and requirements evaluation is a comparison of what is defined at the security requirement description with the implemented security functions. This comparison is simplified in the program and depicted with the '<>' operator in the phase 3 vulnerability identification. This is not just a string comparison, but the evaluation of security functions with their characteristics at a process activity. How such an evaluation could be implemented in detail with a program language is shown in section A.6 with the Prolog program, which determines the adherence of the security objective level for confidentiality, availability and integrity with regard to the implemented security functions. A rule set is used for the evaluation, which represents a knowledge base when the security requirement is adhered to. The user must specify the security objective rating and the ratings of implemented security functions for an EP, PP or CC, after which the program determines whether the security objective is adhered to. Even if the security requirement risk assessment approach (SRA) can be implemented as a formal program, natural language is used to describe the security requirements and as an input for the program. Furthermore, operative security functions have to be identified by the security expert and evaluated against the security requirements. Both procedures identifying security functions as well as the evaluation of security requirements are informal and prone to errors. This is because natural language is used for the description of security requirements (which might be ambiguous) and the degree of operative security functions is determined by documentation reviews (of policies, reports, processes) and interviews by the security expert, for example.

The comparison at Table 6-1in section 6.2.1 demonstrates that the proposed approach is *defining* and *using* security requirements more systematically. Even if the view taken in the comparison would be biased by the belief of the superiority of the proposed approach and therefore disregarded, the comparison between the existing approaches shows that security requirements are currently not coherently defined AND used for vulnerability identification.

In the following a summary about the hypothesis and validation result of the criterion *methods procedure* is provided.

Hypothesis: Security requirements are evaluated systematically for a specific asset by the SRA.

Validation: The comparison (see Table 6-1) between the usage of security requirements in current approaches identified in the literature review using security requirements shows that a coherent definition AND usage of security requirements for vulnerability identification is not the case in current practice. In the SRA, the information assets' security requirements - business security needs - are specified for processing of and containers handling information assets. They are then explicitly evaluated in the business process context. As a result, the security requirements evaluation is more systematic as security requirements are specified and evaluated for single assets in the SRA. Furthermore, the pseudo-code program demonstrates that the approach can be implemented as a program and can be automatised.

6.3. Result accuracy

With result accuracy, the objective was to validate whether the security requirement risk assessment approach is at least as accurate as a current risk

assessment approach (conformity of results). Therefore, an alternative best practice risk assessment approach and the security requirements risk assessment approach were applied by two different assessment teams from the company headquarters, at the same time, at three different insurance entities. Subsidiaries were chosen as their business; IT operations are comprehensible for a security risk assessment and provide a boundary for the assessments. This reduces both the overall complexity and the expenditure of time for the assessment. The results of applying both approaches were used to verify accuracy. It was defined that the validation of accuracy is successful if the security requirements risk assessment approach produces a higher relative accuracy than all identified vulnerabilities of both approaches, and identifies at least the same number of high-rated vulnerabilities. In the following, the context and procedure is described.

6.3.1. Assessments context and procedure

(1) Context

IT security risk assessments are performed by two security experts at entities of a global insurance company, lasting a maximum of one week. The approach used is based on NIST SP 800-30's (Stoneburner et al., 2002b) assessment steps, using COBIT (ITGI, 2007) and ISO/IEC 27001 (ISO, 2005d) control objectives. IT staff are interviewed about security, and security scanning is conducted on systems. Security subject areas are selected based on importance, compliance requirements and common vulnerabilities. Systems used, the underlying infrastructure, and the systems' management are all examined; risks are determined and qualified by their significance (low, medium or high). The approach is performed using the NIST SP 800-30 risk assessment process. Threat-/vulnerability-identification and control analysis are performed by using

vulnerability scanning tools, vulnerability lists and selected COBIT (ITGI, 2007) and ISO/IEC 27001 (ISO, 2005d) control objectives (see appendix A.3), in order to evaluate the implementation of controls. This approach is called the audit/risk assessment approach (ARA).

(2) Procedure

The ARA and the security requirements approach (SRA), proposed in this thesis, were both applied to processes (claims, accounting and underwriting) and systems of three distinct insurance entities. Each of the entities' IT departments operates directory, file, email and application servers, as well as their internet access, and is connected to the corporate network; headquarters provide guidelines for IT security and system standardisation. Each local IT department consists of about 20 to 30 people responsible for service desk, desktops and server operations. Application development does not take place. Business processes were available for the evaluated processes and process activities were similar because of the business model (insurance non-life), but the level of detail and modelling of the processes differed between the entities. Those interviewed did not know whether the information requested was for the ARA or SRA. At the first entity, the ARA and SRA were applied successively, twice, by one assessor. Two different experienced assessors applied the ARA successively, and the SRA was applied by an experienced one and a naïve one, to determine interrupter reliability (Cohen, 1960). At the second and third entities, the ARA and SRA were performed by the same people - now acting as team. The teams did not change and they conducted the assessments subsequently at the three entities. The ARA and SRA teams, which were from the companies' headquarters, had to specify the significance for

the issues identified; furthermore, there was no interaction between the teams after each assessment.

(3) Data - Available business process models

In the environment where the research was performed, a global insurance company, process models are defined for key and support processes. However, the level of detail and currency of process models varies between departments and functions; there is not always a regulatory imperative and a reason for efficiency improvements. The factors relating to the prevalence of business process modelling in a company are the business model (mass production vs. manufacture), profitability (low vs. high margins) and the size/location of the company (non-listed vs. listed and regulated vs. non-regulated). This can be accounted by the fact that process improvements and modelling can help to increase the revenues of companies, as well as to adhere to regulations.

In the following insights are provided as to what business process models were available for the evaluation, which were modelled in Adonis© (BOC, 1995). In the following, a brief overview of the Adonis© notation elements is provided:

- A triangle and cycle represent the start and end of a process;
- Rectangles represent the activities of the process. Each rectangle is labelled with the name of the activity, can contain the activity number and those responsible for the activity as well as can state the used system. Activities are tasks to be executed at that moment and their granularity can vary regarding the requirements of the model;
- Diamonds represent decision points. A decision point has one predecessor and two relations, where one must be true. A decision point can be numbered;

- Arrows between modelling objects (e.g. between rectangles) define the flow of activities and decisions in the process;
- A hexagon represents a trigger that is an event that causes the start of the process;
- A blue triangle with an arrow represents a sub-process. Sub-processes can be used if the same activities are carried out several times in a process or to structure a process.

In Adonis© it is also possible to model risks, controls and the organisation of a company, but these additional elements were not used in the environment where the research was performed.

The process models of the evaluated entities were accessible and could be used for validation testing purposes. However, due to confidentiality reasons, the original process models cannot be presented in this thesis. This is not unusual and other researchers (zur Muehlen, 2007) have also reported that companies are unwilling to provide their business process information for research purposes. Therefore, the original process models have been remodelled to provide a true and fair view of available process models. Any specific details, names or functions have been omitted for confidentiality reasons. In addition, some of the process activities have been consolidated as, in the original process model, this was too specifically modelled with regard to the entity and business type. In the following, the remodelled business process models and the processes purposes are presented and explained. Only the processes that are significantly different at the entities are presented. By significant it is meant that the process flow, activities of the processes, is different. But, in general, the process activities for the three areas examined (underwriting, accounting and claims) at the three entities were

not very distinct, because the examined companies' business and business segment (insurance non-life) is the same, and because global process blueprints were used for organising the business processes at these companies. In addition, the central management and steering of these entities is a further reason why there are only small process differences. The processes available and evaluated are depicted in Table 6-2. A brief description of these is provided afterwards.

Table 6-2: Overview of available and assessed processes at the companies

Processes available and evaluated at companies	Company 1	Company 2	Company 3
Claims processes			
Claims evaluation	X	X	X
Claims notification	X	X	X
Claims payments	X	X	X
Accounting processes			
Claims payments	X	X	X
Commission payments	X	X	X
Booking of new premiums	X	-	-
Booking of changes in premiums	X	-	-
Booking of new and changes in premiums	-	X	X
Underwriting processes			
Contract request and offer	X	-	X
Contract negotiation	X	X	X
Broker business	X	-	-
Customer and broker business	-	X	X

Claims processes

- Claims evaluation (see Figure 6-2): Received claims are evaluated as to whether they are valid; payments are set up and settlements negotiated.
- Claims notification (see Figure 6-3): Claims are received and the claim is pre-checked as well as internally notified.
- Claims payments (see Figure 6-4): Claims payments are checked and authorised by the claims manager.

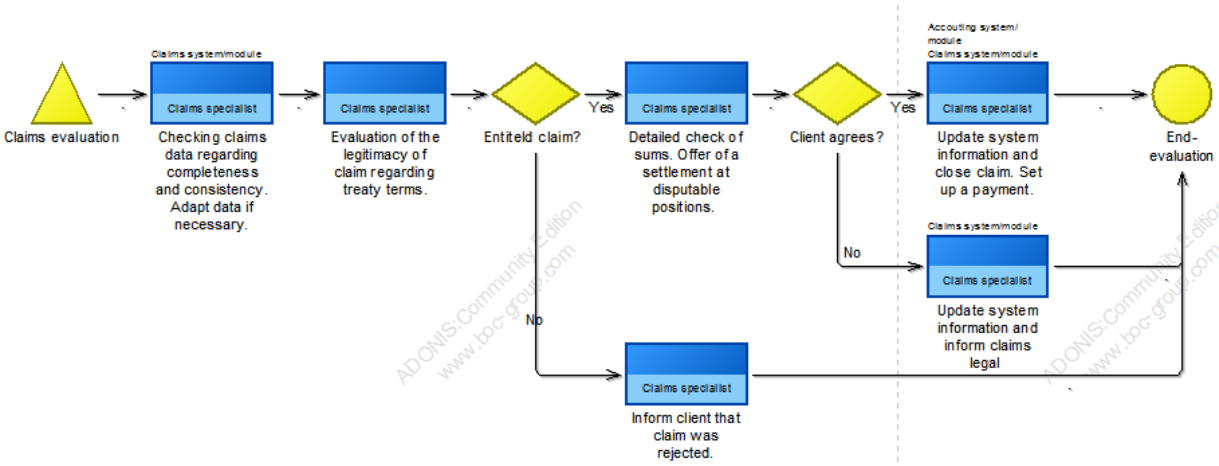


Figure 6-2 Claims evaluation process

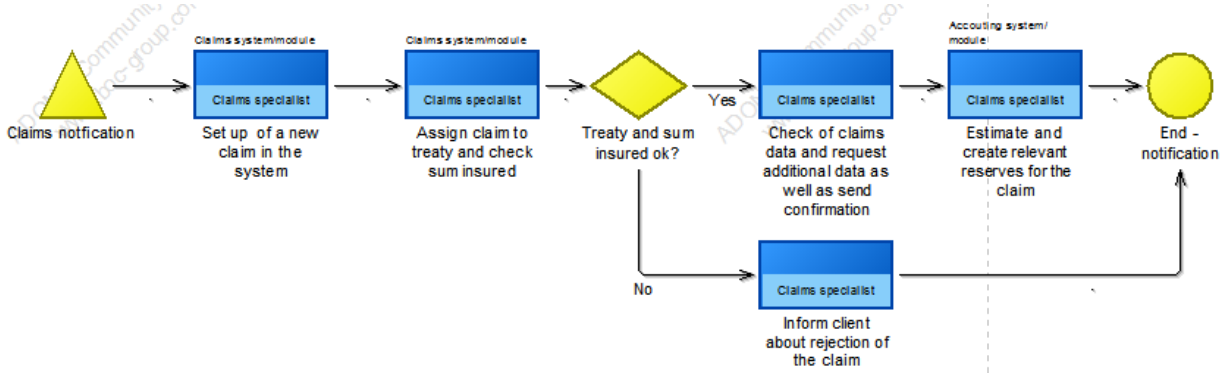


Figure 6-3 Claims notification process

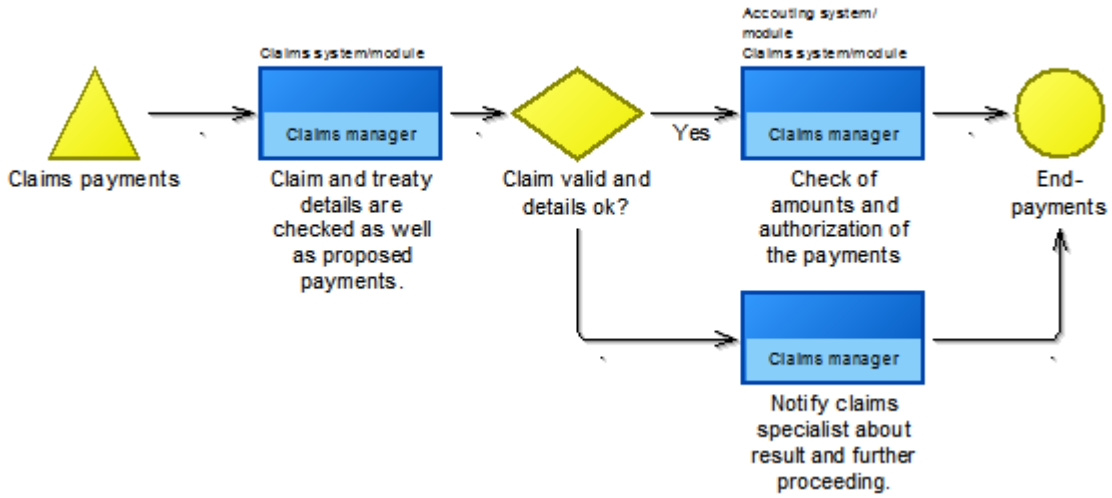


Figure 6-4 Claims payments process

Accounting processes

- Claims payments (see Figure 6-5): The accountant checks the payment details and verifies the bank statements.
- Commission payments (see Figure 6-6): The accountant creates the commission payment and verifies the bank statements. The accountant manager authorises the payments in the systems.
- Booking of new premiums (see Figure 6-7): The accountant sets up a premium booking in the system and matches the daily received bank statement data with the premium booking.
- Booking of changes in premiums (see Figure 6-8): The accountant changes the premium booking in the system.
- Booking of new and changes in premiums (see Figure 6-11): The account decides whether a new premium has to be set up or a change be performed.

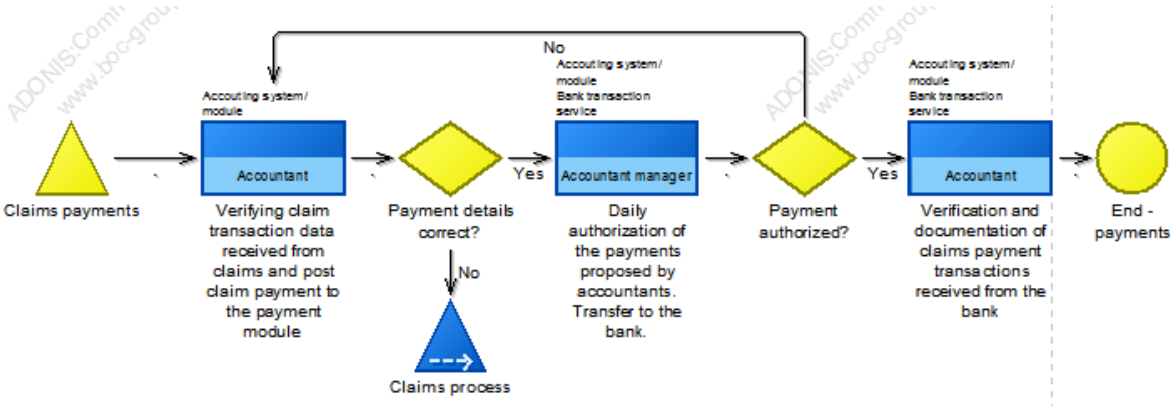


Figure 6-5 Accounting claims payments process

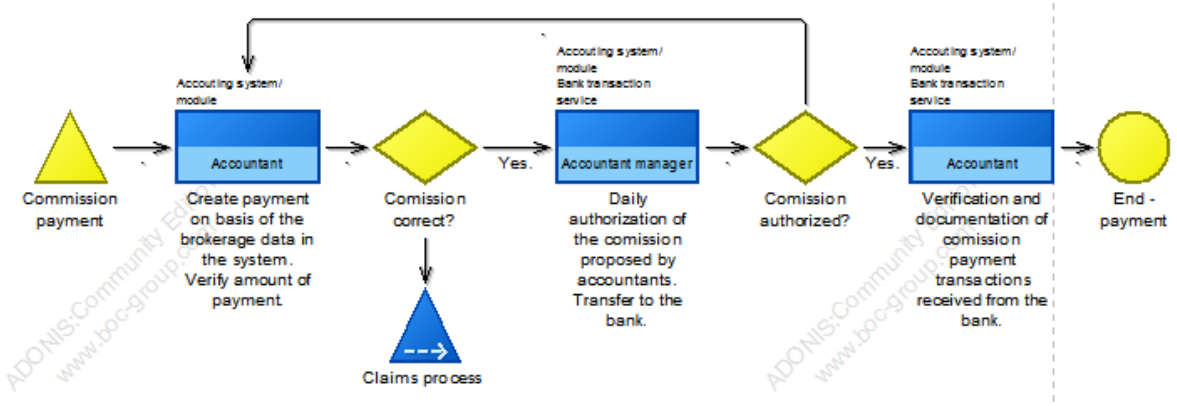


Figure 6-6 Accounting commission payment process

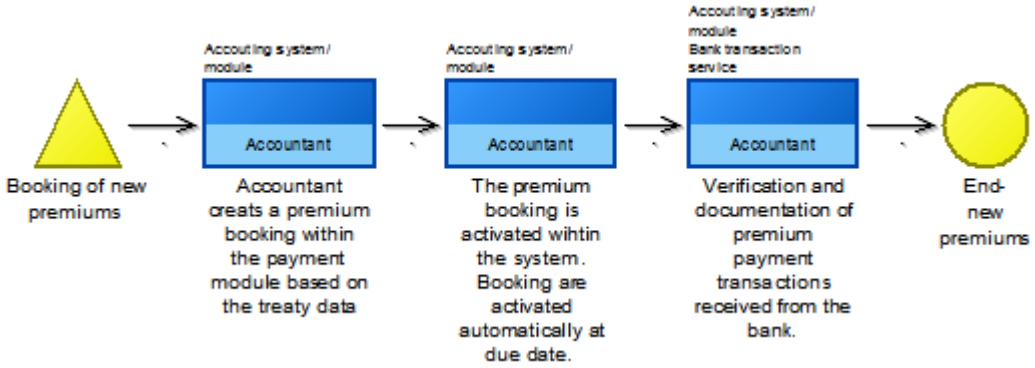


Figure 6-7 Accounting booking of new premiums process

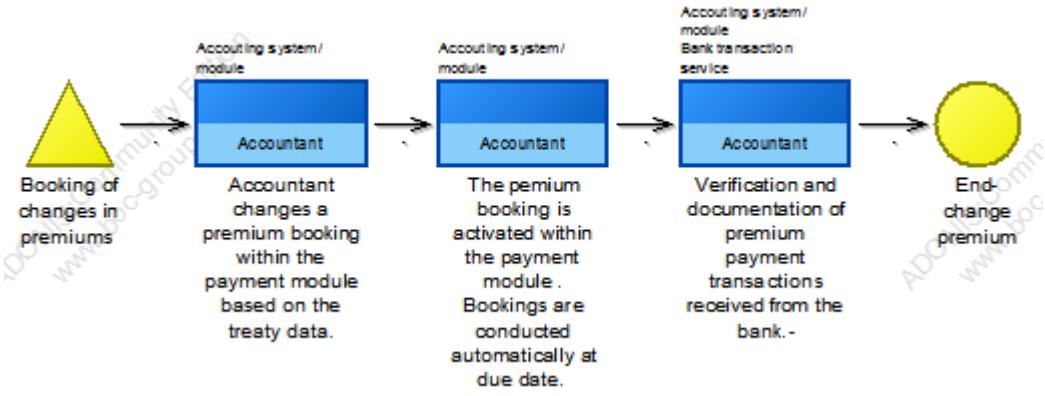


Figure 6-8 Accounting booking of changes in premiums process

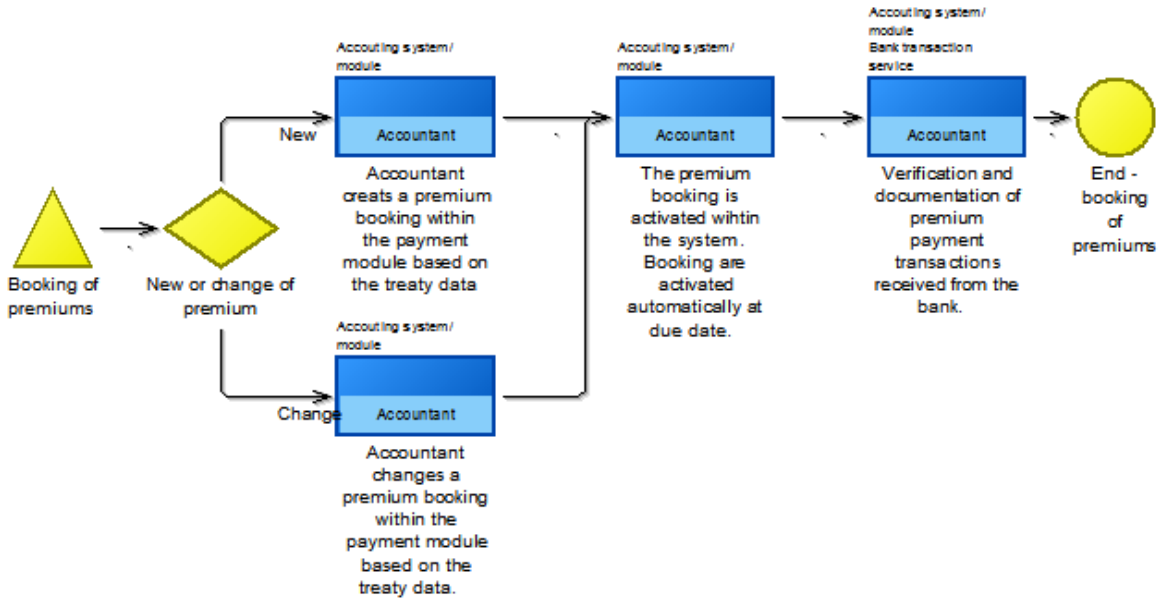


Figure 6-9 Accounting booking of new and changes in premiums

Underwriting processes

- Contract request and offer (see Figure 6-10): The contract request will be forwarded to the appropriate underwriter. The underwriter creates the offer and sends it to the customer.
- Contract negotiation (see Figure 6-11): Underwriter and customer discuss contract details and may change the contract. Contracts exceeding a certain limit have to be authorised by the manager. The underwriter sends the contract to the customer. If the contract is accepted, necessary details and estimation figures are entered and verified in the system. Contract is set active in the system and documentation (e.g. actuary memo) archived.
- Broker business (see Figure 6-12): Underwriter who receives the broker business verifies the broker's registration and the submitted contract details. These details are verified against the Underwriting policy and gain authorisation from a manager when the contract exceeds defined limits or contains special clauses. Underwriter confirms to the broker whether the

contract is accepted, and sets up a new contract in the system. Further contract details are entered into the system and the contract is set as active in the system as well as documentation (e.g. actuary memo) archived.

- Customer and broker business (see Figure 6-13): The customer and broker business process is about creating insurance cover based on the contract request of a customer or broker.

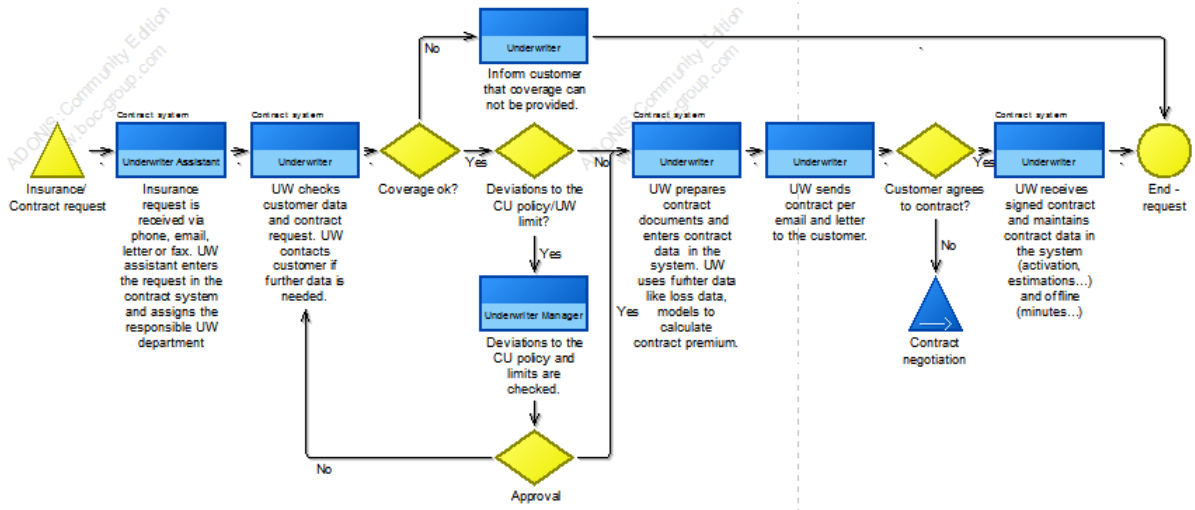


Figure 6-10 Insurance/contract request process

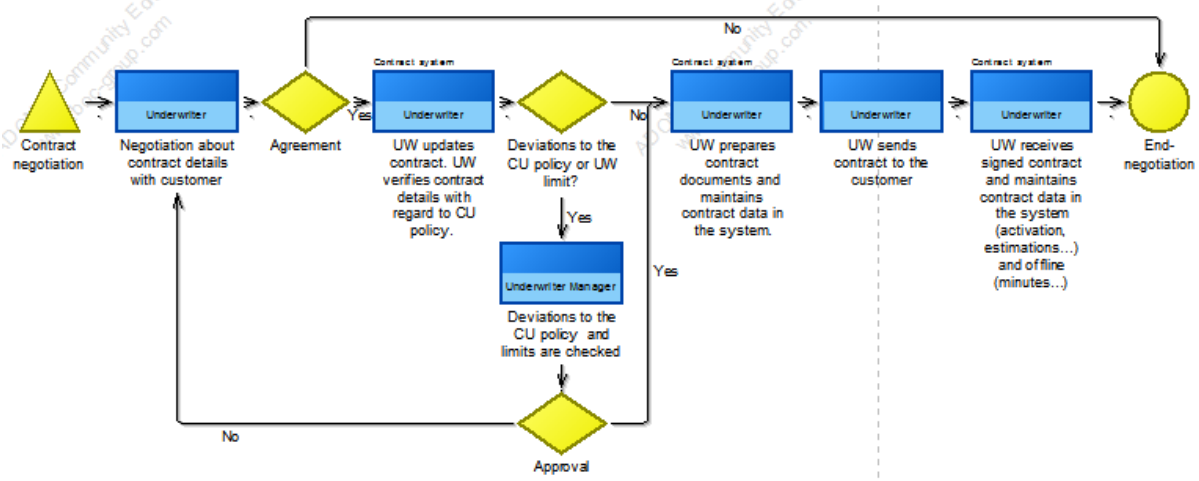


Figure 6-11 Contract negotiation process

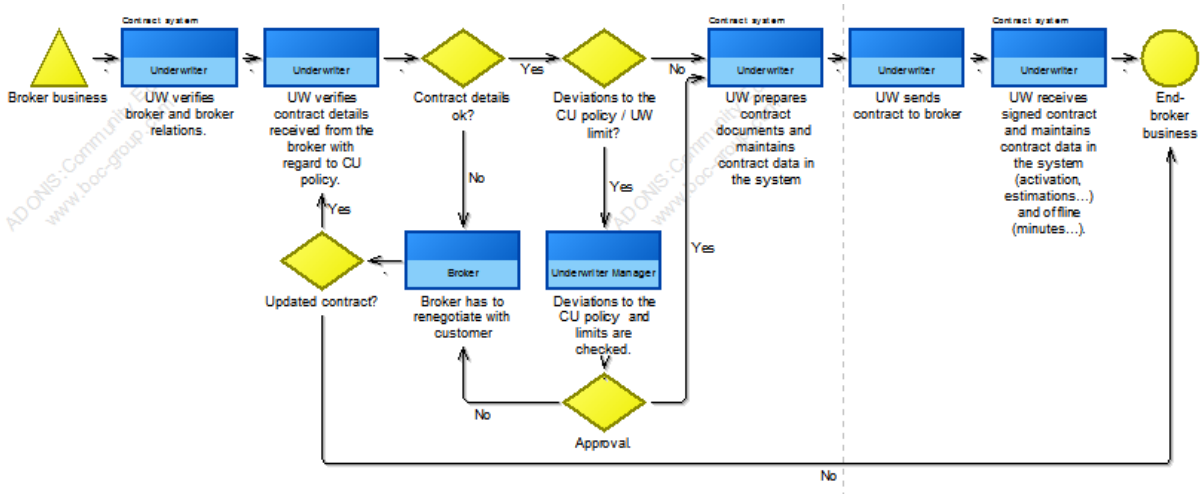


Figure 6-12 Broker business process

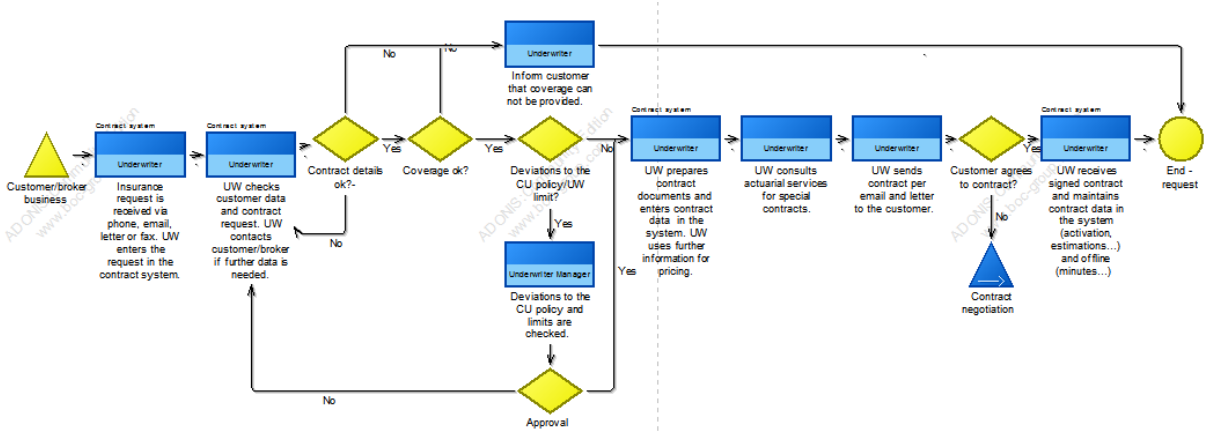


Figure 6-13 Customer and broker business process

6.3.2. ARA assessments execution and results

The ARA has four steps: system characterisation, threat identification, vulnerability identification and control analysis, and likelihood and impact analysis, which follow the risk assessment process described in NIST SP 800-30 (Stoneburner et al., 2002b). In the following, these assessment steps are described in general and the results of the three evaluated entities are presented at the end of this section which were used for validating result accuracy. The detailed assessment results for each entity can be found in the appendix at sections A.4.v, A.4.vi and A.4.vii.

The ARA starts with **system characterisation**. Hardware, software, data and people have to be identified, as well as their criticality or value to the organisation. In the three entities, the contract, claims and accounting application, bank service, and the corresponding information were identified as assets. People involved include claims personnel, accounting personnel and underwriters. For asset identification, the application and network overview were used as well as interviews conducted with IT people. The objective of this step is to determine the assets - the most relevant applications of the organisation for their business - of the company which are included in the risk assessment and are seen as critical for the business. The relevance of the applications is determined by the criticality of the application for the business operation, and whether it contains sensitive (e.g. payment or confidential data) information.

The second step is **threat identification**. All potential threat sources have to be identified. Natural disaster threats, such as tornados, floods and earthquakes, and human behaviour threats from hackers, computer criminals, terrorists/espionage and insiders/disgruntled employees are identified for all three entities. As technical threats, blackouts, fire, earthquakes and chemical pollution are also cited, along with the malfunction of processes. The identified threats are not specifically associated to the assets; they apply for all assets and are to be considered in the evaluation of the assets if applicable. The identified threats drive the selection of evaluated areas and applications at the entities, especially, which parts of the security checklist (see appendix A.3) are used for vulnerability identification at the next step.

As the third step, **vulnerability identification and control analysis** has to be conducted. All weaknesses that can result in security breaches in the system's security procedures, design or operation have to be determined. As a normal procedure, a penetration test and patch scanning are performed. These system testing methods are conducted on infrastructure systems (i.e., network systems, servers and databases) as well as business applications (i.e., the claims, contract and accounting systems). Because of the natural disaster threats, the business continuity documentation and disaster recovery at each entity are examined. The insiders/disgruntled employee threats lead to the review of the access permissions and user accounts of the systems. Natural disaster threats were not considered, as the companies are not exposed. Technical threats like earthquakes, blackouts and chemical pollution were evaluated as unlikely, and fire is treated by sprinkler systems at the entities. Terrorists and espionage were also not considered at the entities because the business is not critical. Later, the information security at the entities is evaluated as to whether business people have enough knowledge about security, and as to whether IT staff handle information securely.

For the identification and analysis of vulnerabilities, a security checklist is used which is based on security best practices such as COBIT (ITGI, 2007), ISO/IEC 27001 (ISO, 2005d) or the ISO 17799:2005 (ISO, 2005c), containing security control objectives (see Table A-5 in the appendix A.3). The security control objectives are used to compare the current implementation with these objectives. Table A-5 shows the typical control objectives used in the ARA for identifying vulnerabilities and risks. For each of the subheadings, a detailed questionnaire is available to determine any vulnerabilities that might exist; this is then evaluated by the assessor if applicable. The evaluated security control objectives for identifying vulnerabilities are selected by the assessors based on the threat identification step

beforehand and the criticality of the assets. The questions aim to identify any vulnerabilities to applications, data, and operational IT processes. For example, asset management, physical and environmental security, information security incident management were evaluated in the assessment at the entities.

As a last step in the assessment, the vulnerabilities' **likelihood and impact are analysed**. The impact and the likelihood of a successful security breach have to be determined based on the criticality of the asset. Therefore, the assessors have determined the significance – a combined likelihood and impact rating – of the vulnerability and rated it as low, medium or high. These significance ratings are based on the assessor's expert judgement. Statistical data or other external data are not used as these data are not relevant or not available for the specific environment.

The assessment results at each company are depicted in Table 6-3, Table 6-4 and Table 6-5. Only at company one, the two assessors performing the assessments had to identify the vulnerabilities separately to compare result reliability. The detailed results of the assessments can be found in the appendix at sections A.4.v, A.4.vi and A.4.vii.

Table 6-3: Company 1 assessment results

Company 1 Results	Assessor 1	Assessor 2	Significance
1. The claims specialist has unrestricted access in the claims system.	Yes	Yes	Medium
2. Data transfer between the bank and the company is insecure as only a weak encryption is used.	Yes	Yes	Medium
3. The operating systems, e.g. of the accounting system misses several patches.	Yes	Yes	High
4. The firewall is not properly configured; websites are not blocked.	Yes	Yes	Medium
5. Unused and active administrative accounts in MS	Yes	No	Low

Active Directory.			
6. Staff are not aware about IS threats.	Yes	Yes	Low
7. There is no appropriate disaster recovery and business continuity documentation.	Yes	Yes	Medium
8. Documents/information were not securely stored in the Claims Department.	Yes	Yes	Low

Table 6-4: Company 2 assessment results

Company 2 Results	Significance
1. Weak VPN connection used by IT staff.	Medium
2. No updated disaster recovery plan.	Medium
3. No testing of the BCM/DR activities.	Medium
4. System access approval process not adequate.	Medium
5. Daily data centre operations procedure not adhered to.	Medium
6. Unused and active administrative accounts in MS Active Directory.	Low
7. Data owner not aware of responsibilities.	Low
8. Unused and active accounts in the HR application.	Medium
9. Paper documents were not securely stored.	Low
10. No audit trail logging activated on database level.	High

Table 6-5: Company 3 assessment results

Company 3 Results	Significance
1. Shared account used for the online banking system.	High
2. The operating systems for various servers are missing several patches.	High
3. No business continuity and disaster recovery plan in place.	Medium
4. Unused and active administrative accounts in MS Active Directory.	Medium
5. No user access lists for local applications.	Low
6. Unused and active accounts in the HR application.	Medium
7. Paper documents were not securely stored.	Low
8. No configuration management existent.	Medium
9. Weak passwords for the backup recovery tool.	Medium
10. The security incident process was not adhered to.	Medium

6.3.3. SRA assessments execution and results

The SRA assessment steps are described in detail in chapter 5.2. It begins with **phase 1 asset identification**. As the most critical processes at all three entities, the claims, accounting and underwriting processes were identified. As information assets, the corresponding data for these processes were determined. At the **phase 2 asset profiling,** the information assets' security requirements have to be specified. The security requirements for the information assets were then reused at the entities as they did not differ much. As information assets, claims, accounting and underwriting data were identified at each entity. Table 6-6, Table 6-7 and Table 6-8 show the security requirements for claims-, accounting- and underwriting information assets with the security objective rating and the security requirements which were used for the evaluation at each entity.

Table 6-6: Claims data security requirements

		Integrity	**Confidentiality**	**Availability**	**IT Security Processes**
Processing	Data	I-L2	C-L3	A-L1	n/a
Containers	Primary Systems	Claims data have to be verified in the system. Data in the system should be protected against unauthorised access and modification. Claims limits needed as well as authorisations. Medium encryption necessary.	Access should be given only to dedicated people of the company Changes have to be logged.	Within one business day	Access Management (authorisations) IT Security Management (Patch Management, Facility) Continuity Management and Disaster Recovery Change Management

	Organisation, People, Process	Personnel entering data should verify their entries as well as the data received. Segregation of duties for claims payments.	People of the departments should be aware of confidentiality.	Core people within one business day.	Access Management IT Security Training IT Security Policy
	Physical	none	Documents should be locked away and disposed of securely.	Within one business day.	IT Security Training Facility Management Business Continuity Management

Table 6-7: Accounting data security requirements

		Integrity	Confidentiality	Availability	IT Security Processes
Processing	Data	I-L2	C-L2	A-L1	n/a
Containers	Primary Systems	Accouting data has to be verified in the system. Data in the system should be protected against unauthorised access and modification. Separation of duties of payments entry and payments release. Medium encryption necessary.	Access should be given only to company people. Changes have to be logged.	Within one business day	Access Management (authorisations) IT Security Management (Patch Management, Facility) Continuity Management and Disaster Recovery Change Management
	Organisation, People, Process	Personnel entering data should verify their entries as well as the data received.	People of the departments should be aware of confidentiality.	Core people within one business day.	Access Management IT Security Training IT Security Policy
	Physical	none	Documents should be locked away and disposed of securely.	Within one business day.	IT Security Training Facility Management Business Continuity Management

Table 6-8: Underwriting data security requirements

		Integrity	Confidentiality	Availability	IT Security Processes
Processing	Data	I-L2	C-L2	A-L1	n/a
Containers	Primary, Systems	Underwriting data has to be verified in the system. Data in the system should be protected against unauthorised access and modification. Medium encryption necessary.	Access should be given only to company people. Changes have to be logged. Approval of policy deviations.	Within one business day	Access Management (authorisations) IT Security Management (Patch Management, Facility) Continuity Management and Disaster Recovery Change Management
	Organisation, People, Process	Personnel entering data should verify their entries as well as the data received. Underwriting and actuarial alignment.	People of the departments should be aware of confidentiality.	Core people within one business day.	Access Management IT Security Training IT Security Policy
	Physical	none	Documents should be locked away and disposed of securely.	Within one business day.	IT Security Training Facility Management Business Continuity Management

At phase 3 vulnerability identification, for each process/sub-process, the EP, PP and CC points in the process are identified and the processing and containers evaluated based on the information assets' security requirements. For each EP and PP, the implemented security concepts - access (AC), authorisation (A), data validation (D) and for CCs encryption (E) - are identified and the adherence to the information assets' security objectives checked. Then, the containers – actors (Org), systems (PiSys) and environment (Phy) - are assessed regarding the security requirements. Finally, the IT security processes specified are evaluated as to whether they are effective and compliant to best practice security processes.

To reiterate, at the first entity, the ARA and SRA were applied successively, twice, by one assessor as explained in section 6.3. At the second and third entities, the ARA and SRA were performed by the same people - now acting as a team.

Security process evaluation

Selected IT security processes, derived from best practice security standards, are evaluated with regard to their implementation and performance. In the sections A.4.i, A.4.iii and A.4.iv in the appendix, the assessment results of the IT processes (ITIL (CCTA, 2007) was chosen as security best practice processes) are included. The column ‘evaluated’ indicates whether the process was evaluated and the column ‘affected data’ which information asset could be affected.

At **phase 4 risk documentation** of the SRA, the risks and vulnerabilities are documented**.** The following tables (Table 6-9, Table 6-10, Table 6-11 and Table 6-12) contain the results of the SRA for the evaluation of claims, accounting, and underwriting processes at the three entities. The result table shows the processes, issues and affected information asset at risk. In addition, the column ‘significance’ was inserted, denoting where the assessors had to determine the significance of the issue identified at the result presentation phase. This rating was introduced for comparison between the proposed approach and the AR approach.

Table 6-9: Result presentation company 1 assessor 1

Processes/Issues – Information asset	Claims data	Accounting data	Underwriting data	Significance
Claims processes – data				
The claims specialist has unrestricted access in the claims system.	X			High
There are no claims limits set up in the system.	X			High

There is no authorisation activity in the process.				High
Paper documents were not securely stored in the Claims department.	X			Medium
Internal oral communication in the claims process was identified as not secure.	X			Low
Accounting processes – data				
Accountants can authorise bookings in the system but should not be able to.		X		High
Data transfer between the bank and the company is insecure as only a weak encryption is used.		X		Medium
Underwriting processes – data				
There is no treaty data verification in the treaty system.			X	Low
Staff are not aware of IS threats.			X	Low
IT Security processes – all data				
There is no appropriate disaster recovery and business continuity documentation.	X	X	X	Medium
The operating system of the accounting system misses several patches.		X		Medium

Table 6-10: Result presentation company 1 assessor 2

Processes/Issues – Information asset	Claims data	Accounting data	Underwriting data	Significance
Claims processes – data				
Unrestricted access in the claims system.	X			High
Claims limits are not reflected in the system or process.	X			High
No secure storage of documents.	X			Low
Accounting processes - data				
Weak encryption is used.		X		Medium
Underwriting processes - data				
Treaty data is not verified in the system.			X	Low
Information is insecurely treated by staff.			X	Low
IT Security processes – all data				
Disaster recovery and business continuity documentation insufficient.	X	X	X	Low
Several patches missing on systems.		X		Medium

Table 6-11: Result presentation company 2

Processes/Issues – Information asset	Claims data	Accounting data	Underwriting data	Significance
Claims processes - data				
The claims specialist is able to release claims without authorisations in the system.	X			High
Process of claims data entry is inappropriate due to missing claims information.	X			High
Used spreadsheets for claims calculation - no access and change controls.	X			Medium
Claims data received were not properly checked.	X			Medium
Underwriting processes - data				
Missing alignment between Underwriter and Actuarial services for contract pricing.			X	Medium
Broker approval process was to work as designed.	X		X	Medium
Missing authorisation for underwriting policy deviations.			X	High
IT security processes – all data				
There is no updated disaster recovery plan.	X	X	X	Low
The BCM/DR activities were not tested appropriately.	X	X	X	Medium
The system access approval process for claims system was not adequate as unlimited access was granted immediately.	X			Medium
The daily procedures in the system operation centre were not processed as required.				Medium
In interviews it was found that data owner are not aware of their responsibilities with regard to applications and the system access.				Low
Some paper documents which contained confidential information were not stored in locked cabinets.	X	X	X	Low

Table 6-12: Result presentation company 3

Processes/Issues – Information asset	Claims data	Accounting data	Underwriting data	Significance
Claims processes - data				
There is no authorisation activity in the claims process.	X			Medium
Underwriting processes - data				
Review and release of quotations in the system were not in line. No system-supported authorisation process.			X	High
Inaccurate data from systems are used in the expected loss ratio studies.			X	High
Inappropriate use of spreadsheets for the calculation of premiums.			X	High
Local actuary model not aligned with central model.			X	Medium
IT security processes – all data				
Shared accounts were found, e.g. for the bank service.		X		Medium
The security patch report revealed that some patches were missing.	X	X	X	Medium
The business continuity and disaster recovery documentation was missing applications.	X	X	X	Medium
IT was not able to provide user access lists for applications.				Low
Paper documents were stored in unsecured lockers.	X	X	X	Low
It was found that a configuration management system did not exist.				Medium
In a few cases where viruses were identified as well as equipment was lost the security incident process was not followed.				Medium
Confidential information was exchanged via the internet.	X	X	X	Medium

6.3.4. ARA/ SRA result interpretation and threats to validity

To compare accuracy, one must know the true value. But as one does not know all existing vulnerabilities (or at least all positive vulnerabilities) in these real world

examples, it is hypothesised that all identified vulnerabilities in both approaches the ARA and SRA represent our relative accurate value (all positives). Whether all existing vulnerabilities have been resolved cannot be verified, as a natural language for security requirements is used and the assessment is a manual process which is error-prone. Table 6-13 categorises the total number of identified vulnerabilities by the ARA and SRA at the three companies, as well as 5-year results of applying the ARA. The *number of total identified vulnerabilities* encompasses all (positive) vulnerabilities that were identified with both approaches the ARA and SRA with identical ones eliminated. At the 5y column, the *number of total identified vulnerabilities* represents all identified vulnerabilities applying the ARA over the last 5 years (from 2007 to 2012). The *number of identified vulnerabilities* is the number of vulnerabilities that were identified with the ARA or SRA. *Relative accuracy/recall* is defined as the number of identified vulnerabilities divided by the number of total identified vulnerabilities. The *overlap between ARA and SRA* is defined as the number of identical vulnerabilities identified by both the ARA and SRA at a company with regard to the number of total identified vulnerabilities. The *number of identified high/medium/low vulnerabilities* in percentage terms is the number of vulnerabilities rated as high/medium/low divided by the number of identified vulnerabilities. The *number of unidentified high/medium/low vulnerabilities* is the vulnerabilities that were not identified with the ARA or SRA with regard to the *total number of identified vulnerabilities* and their significance rating. The 5-year history values at the rows *percentages of identified high/medium/low vulnerabilities* shows the percentages of high/medium/low-rated identified vulnerabilities in 27 assessments of 612 identified vulnerabilities in total. The 5-year history values do not include the current assessment results at the three entities.

Table 6-13: Result comparison

5 y History		Company 1		Company 2		Company 3	
No. total identified vulnerabilities	612	13		17		16	
	ARA	**ARA**	**SRA**	**ARA**	**SRA**	**ARA**	**SRA**
No. identified vulnerabilities	612	8	11	10	13	10	13
Relative accuracy/recall on total identified vulnerabilities in %	n/a	62%	85%	59%	76%	63%	81%
Overlap between ARA and SRA – no. and in %	n/a	6/ 46%		6 / 35%		7 / 44%	
No. identified high vulnerabilities (%)	5%	1 (12%)	4 (36%)	1 (10%)	3 (23%)	2 (20%)	3 (23%)
No. identified medium vulnerabilities (%)	65%	4 (50%)	4 (36%)	6 (60%)	7 (54%)	6 (60%)	8 (62%)
No. identified low vulnerabilities (%)	30%	3 (38%)	3 (28%)	3 (30%)	3 (23%)	2 (20%)	2 (15%)
No. unidentified high vulnerabilities	n/a	3	0	3	1	2	1
No. unidentified medium vulnerabilities	n/a	0	1	4	2	3	3
No. unidentified low vulnerabilities	n/a	2	1	0	1	0	0

Relative accuracy/recall and significance of vulnerabilities is used to determine accuracy of the approach's results. The relative accuracy/recall varies between 17% and 23%, but shows higher accuracy for the SRA in all 3 cases, and is always above 76%. The SRA reliably identifies more (positive) vulnerabilities than the ARA. The overlap of 35-46% of identified vulnerabilities between the ARA and SRA approaches is attributed to the fact that the SRA identifies more process security issues, whereas the ARA is more technically-focused. Using system scanning tools would improve identifying technical issues in the SRA, but tool-based vulnerability identification is time-consuming and momentum is lost (Caralli et al., 2007).

Next, the vulnerabilities' significance was analysed using a distribution analysis. On average, 78% and 71% of all identified vulnerabilities are rated high or medium by the SRA and ARA respectively. The risk significance distribution lies within the expected range of other approaches (Buyens et al., 2007) and the ARA within our

5-year historic data of assessment results, with a higher tendency for low ratings than reported by others (Buyens et al., 2007). This study on risk assessment results (Buyens et al., 2007) and their distribution indicates that risk assessment methods behave differently, especially in the classification of threats. However, the study examined not whether one of the approaches has identified significantly more threats than another approach, as the number of threats was constant. The total number of unidentified vulnerabilities (false negatives) shows that the ARA missed 8 (17%) and the SRA two (4%) high-rated vulnerabilities, out of a total of 46 (positives). With the SRA approach, a high accuracy on business process-related issues, as well as on high-rated vulnerabilities can be achieved. Any other developed approaches would not perform significantly better, as they are based on information security standards using security best practices and vulnerability lists for vulnerability identification, like in the ARA approach. This is also true because these approaches do not evaluate asset-specific security requirements. With the SRA, there are 15-28% low-rated vulnerabilities which were not expected, because of our security requirements definition only identifying significant ones.

An inter-rater reliability analysis using Cohen's Kappa (Cohen, 1960) was performed for the ARA and SRA results at company one, determining consistency between raters, and was found to be 0.45 for the SRA and 0.51 for the ARA. These ratings represent a moderate agreement (Landis and Koch, 1977) for both raters in both approaches, indicating that the consensus was more than due to chance. In general, it is difficult to attain an almost perfect agreement between raters for risk assessments; the risk assessment procedure to be followed is an informal one, relying on the assessors' experience and natural language descriptions of vulnerabilities and security requirements.

For the comparative analysis between the ARA and SRA approach results, one risk identifier was created and assigned. This could have affected both approaches, assuming that it holds no advantage for either one. The proposed approach in this thesis was only tested in one specific business sector insurance non-life at three companies. Therefore, the generalisation of results may be limited to some degree. But the sample size used is not unusual for this type of research, as often only one real world example is used by other researchers for validation. Furthermore, it was found that case studies with a large number of business process models are not available, and companies are often unwilling to publish their business models for research (zur Muehlen, 2007).

A security checklist based on COBIT (ITGI, 2007) and ISO/IEC 27001 (ISO, 2005d) was used in the ARA and a rule set for evaluating the security object level in the SRA. Both tools which were used for the identification of vulnerabilities have not been evaluated as to how efficiently they can identify any vulnerabilities, or whether there is an advantage for one of the approaches. The same could be true for the ARA and SRA procedures for identifying vulnerabilities. This efficiency identifying most (relevant) vulnerabilities could also cause a better accuracy of results. However, as the approaches were applied three times, the assessors were more familiar and experienced with the ARA approach, and the assessment results were quite similar, so this should not be an advantage for the SRA approach.

When applying the SRA, the assessors already had extensive experience in doing risk assessments in the applied business domain. Therefore, their experience and

knowledge may have unknowingly influenced the results. It is not known whether the results would have been different if the assessors had not been familiar with the SRA or ARA, or had less knowledge in risk assessments. On the other hand, professional IT security experts have experience in different domains and approaches and also use that in their risk assessment, without being aware of it. Risk assessors underlie subjectivity with regard to the risk rating. Furthermore, the SRA assessors reported that the approach was no more complex to apply than the ARA approach. Complexity was rated by the number of activities/ steps of the approaches and whether they are readily understandable. However, the SRA assessors criticized that identifying entry, process and communication points, applying the rule set and consolidating results is work-intensive. But with automation of the SRA approach, manual and work-intensive steps could be reduced.

In the following a summary about the hypothesis and validation result of the criterion *result accuracy* is provided.

Hypothesis: The SRA is accurate in determining vulnerabilities: in particular, the SRA produces a higher relative accuracy referred to all identified vulnerabilities (positives) of the ARA and SRA, and at least identifies the same number of high-rated vulnerabilities.

Validation: This hypothesis was tested at three distinct insurance entities applying both the ARA and SRA, in parallel, and by different assessment teams. With the SRA, security issues were identified 17% more accurately (true positive vulnerabilities). Especially business-related security issues were identified more accurately, and these are more significant risks for the company (Khanmohammadi and Houmb, 2010). The SRA identified the same number of

high-rated vulnerabilities as the ARA at all entities. The total number of unidentified vulnerabilities (false negatives) shows that the ARA missed 8 (17%) and the SRA two (4%) high-rated vulnerabilities, out of a total of 46 (positives). With the SRA, a high accuracy was seen on business process-related issues, as well as high-rated vulnerabilities, in comparison to the ARA, which uses security best practices for vulnerability identification.

6.4. Method capability

To demonstrate that vulnerability identification errors occur (false positives) and can be resolved by using security requirements, a quasi-experiment was conducted included in a survey about security risk assessment procedures at an information security conference of professionals in the 'D-A-CH' region (Germany, Austria, Switzerland). The complete survey and its results can be found in the appendix at section A.1. The conference was about information security trends, threats and assessments. In the quasi-experiment (see appendix section A.1.iv) participants had to assess risks using different sets of information. Both the survey and quasi-experiment were administrated by the thesis author.

6.4.1. Quasi-experiment design and procedure

In the quasi-experiment, each third of all conference participants (in total 55 security professionals) had to identify risks of a real world example based on threats; based on threats and a business process model; and based on threats, security requirements and a business process model respectively. The participants had to determine risks and their impact based on the information available. In cases A and B there were two predefined risks, and in case C there were three additional predefined risks (see Table 6-14, risks 1 to 5). All were described in the

risk (risks 1 and 2) and security requirement (risks 3,4 and 5) description. In this quasi-experiment, the precision and accuracy of determining predefined and additional vulnerabilities by the participants' is studied. A high number of additional risks identified by the participants, but not described in the risk/threat description, would indicate that vulnerability identification errors occur. A higher accuracy of identified predefined vulnerabilities as well as a decrease of additional identified risks at case C, would indicate that vulnerability identification errors can be resolved with security requirements. The following information was provided to the survey participants in case A, B and C:

Risk situation description (provided in cases A, B and C):

A company sells all its goods through an online shop. Approximately 1000 orders per day are processed and only orders that are higher than €25 are processed and stored in an online CRM system. If the customer wants to pay by credit card or by bank transfer, the payment data is forwarded to a bank which processes the payment transaction. The online shop is important for the company, as all sales are generated through it. In a security analysis, it was found that via the input fields in the online shop (CRM system), database content can be changed. In addition, customer data and payment data transmitted are not encrypted. All employees of the ordering process have access to read and order data in the CRM system. The CRM system was not available in the last ten days, on two occasions for one hour each, due to a system failure caused by maintenance work.

Business Process model "Sales" (provided in cases B and C):

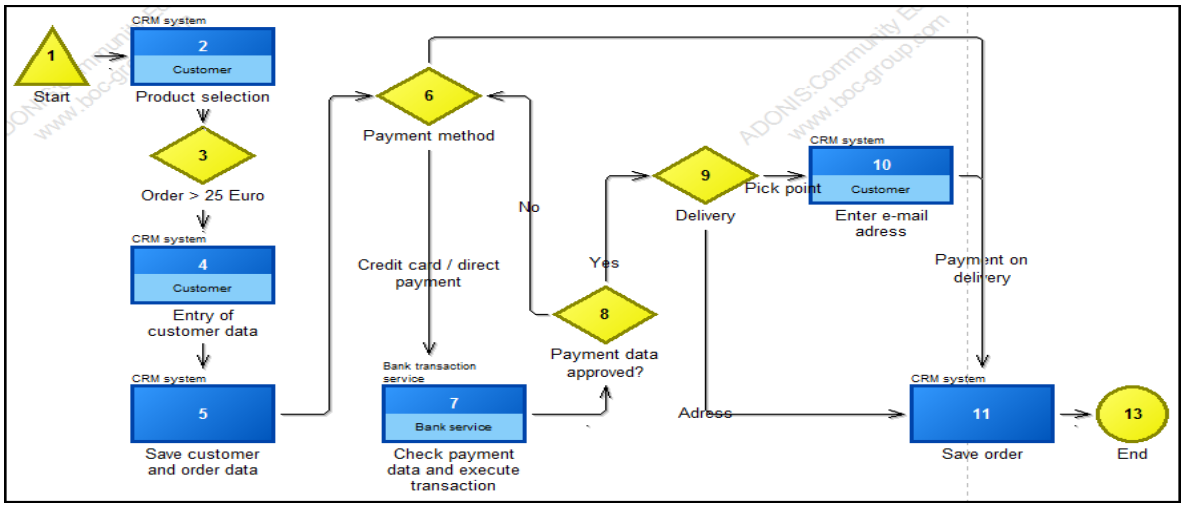


Figure 6-14 Business process example order process

Security requirements description (provided only in case C):

The business process "sales" is classified as critical for the operation of the company. For all customer, order and payment data, the confidentiality and integrity must be ensured and IT systems should not exceed 15 minutes per day of unavailability. In the business process "invoice", it was specified that only employees of accounting may view all order data. Saved transactions (orders) in the sales process are to be authorised after saving the order, by a member of the sales process and to be transmitted to the “invoice” process.

Quasi-experiment procedure

The quasi-experiment was conducted with all 55 security professionals of the conference in a closed room; for the completion of the risk assessment 30 minutes were available. A closed room was used so as not to disturb participants by any non-participants, or those leaving the experiment early. Interaction with others was not allowed and the survey instructor’s involvement was limited to answers on how to fill out the template. Each third of the participants was provided randomly with

one of three alternative sets of information representing the dependent variables of the experiment. In case A (12 of 20 distributed forms were evaluable) a risk/threat description was provided, in case B (13 of 15 distributed forms were evaluable) the risk/threat description with a business process model was provided and in case C (11 of 20 distributed forms were evaluable) the risk/threat description with security requirements and a business process model were provided. All participants were security professionals responsible for information security in their companies, or security consultants, and therefore knowledgeable about security risks. In addition, in the survey conducted before the quasi-experiment, participants had to answer various questions about risk assessments and therefore should be aware of concepts used in the experiment.

6.4.2. Quasi-experiment results

For each case, it was analysed how accurately the participants identified the predefined risks (true positives), and how many other risks (false positives) were identified. The results are shown in Table 6-14. Furthermore, the risk rating assigned by the participants to the predefined risks as well as to other risks in all three cases was analysed - see Table 6-15. In case C, participants only had to specify whether the risk is acceptable or not based on the security requirements provided. In the result presentation the term risk is used synonymously with vulnerability, as threats were not identified separately. The results are as follows:

Table 6-14 Quasi-experiment risks identified by participants

	Identified Risks in percentages		
Predefined Risks	**Case A**	**Case B**	**Case C**
1.Data integrity (in case A, B and C)	100%	100%	73%
2. Data confidentiality (in case A, B and C)	67%	85%	91%
3. Process design data confidentiality (only case C)	8%	0%	45%
4. System availability (only case C)	100%	85%	100%

5. Process design authorisation (only case C)	0%	0%	20%
6. Other identified risks (in case A, B and C)	75%	77%	55%

Table 6-15 Quasi-experiment risk impact evaluation by participants

	Risk Rating		
Predefined Risks	**High**	**Middle**	**Low**
1. Data integrity - Case A	83%	17%	0%
1. Data integrity - Case B	85%	15%	0%
2. Data confidentiality - Case A	75%	13%	12%
2. Data confidentiality - Case B	55%	45%	0%
4. System availability – Case A	58%	34%	8%
4. System availability – Case B	73%	18%	9%
6. Other identified risks - Case A	44%	56%	0%
6. Other identified risks - Case B	10%	50%	10%
	Acceptable Risk		
	No		**Yes**
1. Data integrity - Case C	88%		12%
2. Data confidentiality - Case C	90%		10%
3. Process design data confidentiality – Case C	100%		0%
4. System availability – Case C	100%		0%
5. Process design authorisation – Case C	100%		0%
6. Other identified risks - Case C	67%		33%

6.4.3. Result interpretation and threats to validity

In case A, 100% and 67% of the participants identified predefined risks one and two respectively (see Table 6-14). All participants (100%) identified an availability risk that was not present; three out of four identified multiple other risks that were not present. In case B, predefined risks one and two were identified by 100% and 85% of participants, respectively. The non-existent availability risk was now only identified by 85%, but three out of four participants also identified multiple other risks that were not present. In case C, 75% and 91% of participants identified the predefined risks one and two respectively, and 45%, 100% and 20% recognised risks three to five. ‘Other identified risks’ were noted by 55% of the participants. One could argue that the risk description was misleading - especially the

availability problem description - or that variants of risks were identified by the participants not related to the data integrity risk, for example, leading to vulnerability identification errors. But even if we omit the availability risk, other risks were identified. The issue that participants identified variants of risks not properly related to predefined risk was considered. All identified risks were recorded per participant and associated with one of the six predefined risks. Only these risks which could not be associated with one of the predefined risks were associated with the other identified risks, but only one other identified risk per participant was counted.

The experiment risk results show that in all three cases, ‘other identified risks’ (one or more) were identified by between 55% and 77% of the participants (see Table 6-14). In case B, the process model information supported study participants by identifying vulnerabilities more precisely; e.g. the increase of 18% in risk 2 and a decrease of 15% in risk 4. In case C, where security requirements were provided additionally, the identification of non-existent risks decreased (from 75% to 55%), but the added complexity negatively influenced the risk identification rate. Risk 5 was identified by 20% of participants and in risk 1, the rate decreased to 27% due to the need to identify multiple risks. However, in all cases, more risks were identified as existent in the information provided, because assessors used tacit information and knowledge about security requirements and risk/vulnerabilities. This was evident by the participants identifying and describing risks differently.

The analysis of the risk impact evaluation of the participants per predefined risk (and ‘other identified risks’) in cases A and B (see Table 6-15) illustrates that assessors tend to rate vulnerabilities as high or medium. Especially risks rated as

medium need a further analysis and prioritisation by the security expert and management, as to whether security functions have to be implemented. In case C, participants had to rate only whether the risk was acceptable or not, according to the security requirements definition. This follows the concept of ‘security needs’ - a risk is only a risk if there is a requirement. This rating, together with the security requirements, helped participants to decide whether the issue is a risk/ vulnerability for the company; this is reflected in high ratios for not acceptable risks. A further analysis of the ‘Other identified risks’ and their risk impact rating shows that, in cases A and B, the impact of other risks was mostly rated as medium or high; they were perceived as risks/vulnerabilities. In case B, some of the other risks were not rated by participants and therefore were not included in the statistics. In case C, 33% of the other identified risks (55%) were rated as acceptable. This reduces the effective rate of other identified risks to 36%. This result supports also the statement that vulnerability identification errors can be resolved with security requirements.

The response rate was 60% in cases A and C but 87% in case B. Some of the forms were not filled, or were completed in a way so that results were not usable. The process model supported the participants to be able to evaluate risks, represented by a higher return rate. Case A was unusual as the risk description was represented clearly and was easy to understand. The low response rate in case C can be attributed to the complexity – three sets of information that have to be considered together – of the risk assessment example; the variable of the quasi-experiment had to be changed.

In case C, the variable of the quasi-experiment, the predefined risks, caused complexity. The internal validity of the experiment is threatened by this complexity. But, additional risks had to be created in case C in comparison to A and B, in order to verify whether participants can really identify vulnerabilities by the security requirement definition and not only by the risk description. This caused the accuracy of risks 1 and 2 to decrease slightly, as well as other risks being identified in case C. One could assume having added additional risks is the reason for the decrease of identified additional risks. But the total number of all identified risks decreased by almost 10% in case C, indicating a higher accuracy. With the additional risks in case C, it is also demonstrated that participants were able to identify vulnerabilities only based on security requirements and business process model information.

The error rate defined as non-existent risks (false positives) identified per participant in the experiment was: in case A 2.1; in B 1.6; and in case C 0.55. A participant in case A identified 1.5 times as many non-existent additional risks than one in case C. The business process model and security requirements provided helped the participants to identify risks more accurately - identifying positive risks in the experiment.

The experiment participants – security professionals – had various competence levels in risk analysis and security assessments, and therefore were well aware of security risk concepts. Their competence level in security risk analysis was not further determined, but the experiment results and survey results showed their general understanding of security risk concepts. The synonymous usage of the term risk and vulnerability could have influenced their interpretation and thus the

results. However, a discussion with the participants about differences of risk and vulnerability and using security requirements for vulnerability identification following the quasi-experiment did not reveal any issues about synonymous usage of terms as also the impact for a risk was required in the experiment.

In the following a summary about the hypothesis and validation result of the criterion *method capability* is provided.

Hypothesis: Vulnerability identification errors occur in practice and by explicitly considering security requirements in an assessment, vulnerability identification errors can be resolved.

Validation: The quasi-experiment shows that vulnerability identification errors occur in practice. Up to 77% of the study participants identified additional risks (false positives) in cases A, B and C which were not present in the example provided. Furthermore, security requirements and business process model information helped study participants by identifying vulnerabilities more precisely, leading to a decrease of approximately 20% in vulnerability identification errors (false positives). If the impact ratings of these additional vulnerabilities are also considered by eliminating acceptable vulnerabilities, then vulnerability identification errors were reduced by 39%.

6.5. Lessons learned

With the validation, experience was gained about a security requirements-based risk assessment approach for vulnerability identification which is presented below.

Security requirements elicitation

In general, security requirement elicitation was not very difficult for the information assets, as the context the business process and activities of the assets was

described. The business context helps to determine security requirements as information about the business goal, the input and output of the process, the process activities' interaction as well as the actors is available. However, the detailed specification of requirements was not straightforward, as knowledge about the security requirement to-be and security functions are necessary. Existing security best practices can help to derive security functions. In addition, the more specifically the security requirements were defined, the easier their evaluation was. Furthermore, security requirements have been reused as the specification was quite similar and has not to be changed.

Identification of vulnerabilities

It was recognised that issues related to system implementation, process design/implementation and the organisation were identified more easily with the SRA, whereas technical issues were identified more successfully with the ARA. This shows up strongly in the results. However, sometimes the comparison of the requirement with the current implementation and their evaluation was difficult - especially to determine the extent to which security functions are implemented and whether they were implemented accurately. There is some scope for inaccuracies whether the implementation corresponds with the requirement, particularly when the requirements are described as high-level. Technical issues, like system vulnerabilities, can be determined by the SRA by checking corresponding security processes. However, the identification of technical risks was sometimes tough; other techniques like security testing had to be applied. An example for this is checking system vulnerability patches, where the assessors had to use a security scanning tool instead of evaluating the documentation in order to verify the performance of the process - no system patch report was available.

The assessment process

The security requirements based assessment process is still an informal one, because security requirements and functions have to be defined, identified and evaluated by a security expert. For example, the extent of the security function implementation and determining the security function configuration at the process activities need expert judgement. The ratings assigned to, say, process points and the fulfilment of security objectives or requirements needs interpretation and could be influenced by the perception of the security expert.

Furthermore, often the system, actor or organisation has to be evaluated several times at the different EP, PP and CCs in the business process. This causes reoccurring evaluation work for the assessor, who could tend to copy and paste the results. In addition, the reasons why a process point does not adhere to the security requirements must be documented separately as the evaluation result does not reflect the underlying issue. This means the result documentation has to be immediately updated with the identified issues.

Beyond that, the rules base which is used for the evaluation was derived from the security objective ratings, as well as from company specific security definitions and guidelines. These rules were validated by the companies' security policies and publically available security best practices. The rule base can and might be adjusted if used at other companies, as some rules might not apply to other companies. Some borderline cases were recognised where the rules tend to classify the implementation as insecure or secure - this might be wrong in a given situation. Therefore, the rules' result had to be questioned in some cases and even manually corrected. Before an assessment is started, the rule base should be verified with regard to company-specific security guidelines.

Risk result presentation

The presentation of the business process and whether an information asset is threatened helped managers to understand what assets are endangered after the assessment. This presentation of risks was found to be more helpful as the risk impact representation in current approaches, as was confirmed in the survey. In addition, fewer discussions were recognised on risk mitigation and countermeasure implementation; this is because the security requirement violation is backed up by business security needs or security policies which were not called into question. In the ARA, low/medium or medium/low risks were discussed with managers and sometimes not rectified. These discussions are due to the representation of the risk and the possibility to interpret results. One has to be aware that any acceptance of identified risks by managers would change the company's security level. The modification of the security level by accepting risks will become more apparent in the SRA, because this would directly lead to changes in the company's security requirements. Furthermore, it was experienced that there are different factors implicitly considered by people representing constraints to countermeasure implementation.

Frequency: Countermeasure implementation is dependent not only on costs, impact and probability, but also on frequency. But the frequency in a period of time is generally not specified in risk assessment results.

Cost objectives: The implementation of measures depends on a company's internal cost objectives; personal or departmental objectives may not be accomplished. Furthermore, measures that are not planned in the current year's budget may not be implemented immediately.

Prioritisation: Business-critical projects' or daily operations' security issues have a higher priority than proposed countermeasures, as an event has materialised.

Risk attitude and perception: The perception of risk by people influences countermeasure implementation. Personal experiences as well as the risk attitude of a person - risk-taker vs. risk-aware person – have an impact on risk decisions which are not apparent.

6.6. Chapter summary

With the validation criteria *method procedure, result accuracy and method capability* the objective was to demonstrate that a security requirements-based approach (SRA) systematically determines vulnerabilities and can resolve vulnerability identification errors (false positives). With *method procedure* it was shown that a coherent definition AND usage of security requirements for vulnerability identification are not present in current practice and therefore, the SRA is more systematic. With *result accuracy* it was demonstrated that with the SRA, security issues were identified 17% more accurately regarding all identified vulnerabilities of both approaches – the ARA and SRA. With *method capability* it was demonstrated that vulnerability identification errors occur in practice and security requirements and business process model information helped to decrease identification errors by at least 20%.

Chapter 7 – Conclusions and Future Work

In this chapter, a summary of the research contributions is presented in section 7.1. Section 7.2 describes the limitations of this study, and section 7.3 discusses recommendations for future work.

7.1. Research contributions

The research objective was to utilize security requirements at the vulnerability identification phase of security risk assessments for resolving vulnerability identification errors (false positives). Therefore, in this thesis, three research contributions were presented to achieve the objective. Firstly, vulnerability identification errors do occur and security requirements are not explicitly evaluated to identify vulnerabilities accurately. The discussion on problems of risk assessment approaches (section 3.4) shows that vulnerability errors occur because of uncertainty about events, threats and probabilities used in the assessment procedure. This was also reported by participants of a survey performed at an information security conference (see section 3.4.2), characterising assessments as subjective and error-prone, and further confirmed in the quasi-experiment (see section 6.4). Furthermore, the literature review (chapter 3) identified that in current risk assessment approaches for organisations, asset-specific security requirements are not explicitly evaluated to identify vulnerabilities accurately, but rather used for determining the impact of vulnerabilities. Therefore, a statement about security - the true, accurate value of a measurement system (Viera and Garrett, 2005) - cannot be made, because the security itself is not explicitly evaluated in assessments.

Secondly, an extended information security model was presented in chapter 4.1; this showed the relationships between risk-, asset- and security-related concepts for a security requirements-based definition of risk. Security requirements are linked to risks, vulnerabilities, business security needs, security controls, assets and risk treatment. Based on these relations, a security requirement-based definition of risk was provided which allows for the accurate identification of vulnerabilities and risks by using security requirements – business security needs. Furthermore, the extended information security model relates risk treatment and asset-related concepts via risk *and* security requirements, not only via risks as in other models. The extended model can help to better understand the relationship between risk-, asset-, security requirements- and risk treatment-related concepts and thus can help to achieve a better integration of these concepts in risk assessment approaches.

Thirdly, vulnerability identification errors can be resolved by a security requirement-based approach. Security requirements and business process model information help to decrease vulnerability identification errors, as shown by the quasi-experiment of chapter 6.4. Vulnerability identification errors (false positives) decreased by approximately 20% when using business process models and assessing security requirements. If the impact ratings of these additional vulnerabilities are also considered by eliminating acceptable vulnerabilities, then vulnerability identification errors decreased by 39%. The error rate - defined as the rate of non-existent risks/vulnerabilities (false positives) identified per participant – decreased, while the accuracy on (positive) vulnerabilities increased by using the business process model as well as security requirement information. Furthermore,

the validation work of chapter 6.3, applying the ARA and SRA by two different assessment teams at three insurance entities, shows that security issues were identified at least 17% more accurately (true positive vulnerabilities) with a security requirement-based approach, in comparison to a security best practice approach. Accuracy was defined as the number of identified vulnerabilities of the approach divided by the number of total identified vulnerabilities (all positives) by both approaches. In particular, business-related security issues were identified more accurately, and the SRA missed only two of all high rated vulnerabilities, in comparison with eight missed by the ARA - and these are more significant risks for the company (Khanmohammadi and Houmb, 2010).

Furthermore, with the pseudo-code program (see section 6.2.2), the UML model (see appendix A.2), and Prolog program (see appendix A.6), it was demonstrated that a security requirements-based approach using business process models can can be implemented as structured procedure. This proof of concept - implementing the proposed security requirement-based approach as a program - illustrates that the assessment procedure and evaluation can be automatised and is applicable.

Because of the results in this thesis, it is suggested that the explicit evaluation of assets' security requirements is incorporated into risk assessments, especially in the risk identification phase, to identify true positive vulnerabilities and to resolve vulnerability identification errors (false positives and false negatives). This is different to current approaches where security requirements are used only for determining the impact of vulnerabilities.

7.2. Limitations

The work in this thesis has some limitations, particularly regarding the usage of security requirements and business process models for resolving vulnerability identification errors. The limitations noticed are as follows:

The definition and specification of security requirements both need public knowledge about threats and vulnerabilities; if a specific threat or vulnerability is not commonly known, it is unlikely to be identified. This is because the security expert or any security testing tool would not identify the vulnerability, and it might not thus be properly reflected in the security requirement specification. However, the same is true in any vulnerability identification procedure, if vulnerabilities are not known at all. In all methods, only known vulnerabilities can be identified, as the matching principle is applied to identify vulnerabilities.

Security requirements can be defined generally, but the identification of vulnerabilities is more efficient if security requirements are specified more precisely with regard to threats and vulnerabilities. Vulnerability identification is dependent on the precise definition of security requirements, which can be set by the business process owner or security expert. However, in the proposed approach there is no formal verification process as to whether the specifications are correct and comprehensive. For the verification of security requirements, the frameworks of other researchers like Herrmann and Herrmann (2006), who used graphical concepts to specify requirements, could be used.

The business process models used for the approach have to be available and up-to-date, so that they represent current business operations. Any inconsistencies between the modelled processes and actual business operations can be identified to some degree with the SRA, as the evaluation is based on available documentation and interviews. However, if the modelled process does not correspond to businesses operations, vulnerabilities cannot be identified correctly. But, in an evaluation, discrepancies between the process model and the current implementation would at least be indicated, but the vulnerabilities would not necessarily be resolved.

The information security model was developed based on those models presented in chapter 1.2, and is the foundation of the security requirements-based risk definition. This risk definition does not include an event or impact statement, as the non-adherence to the security requirements is not intended and is expected to cause harm to the organisation. By this definition, the focus is on the correct security function implementation protecting information and representing vulnerabilities, rather than on identifying scenarios of what could go wrong and determining their impact. This also leads to the risk assessment steps, risk identification and analysis, being combined. Furthermore, this definition presents a hurdle for low-rated vulnerabilities, and as a consequence they will not be identified as a risk or vulnerability for the organisation. Therefore, vulnerabilities having a low impact may not be completely identified.

The validation of the SRA with testing regarding the criterion result accuracy was limited to the insurance business sector with a limited number of business process models. No case study with a large number of business process models over

different business domains, or any public information about specific security issues of business domains, could be identified in the literature. Therefore, the results of this thesis are limited to the applied business domain. Furthermore, the risk assessment result comparison was limited to a best practice approach based on NIST SP 800-30 (Stoneburner et al., 2002b) with assessment steps using COBIT (ITGI, 2007) and ISO/IEC 27001 (ISO, 2005d) - security best practices with which the assessment teams were familiar. Other developed approaches are likely to perform equally as well as the ARA approach, as they are based on information security standards using security best practices and vulnerability lists for vulnerability identification, but none were tested. In addition, relative accuracy (all positives) was defined by the number of identified vulnerabilities in both approaches. Using this figure for accuracy might affect result interpretation, as this figure for all positives could contain false positives and omit false negatives. However, in real world examples it is virtually impossible to determine all positive/negative vulnerabilities (or at least all positive vulnerabilities) and in the SRA, true positive vulnerabilities were solely determined by asset-specific security needs and not by organisation-unspecific security best practices (as in current proceedings).

The validity of the quasi-experiment, showing that vulnerability errors occur and can be resolved, was threatened by the selection of the experiment group and the complexity of the information provided. However, a prerequisite for the experiment is that the experiment group has knowledge about information security risk analysis, otherwise they would not be able to determine vulnerabilities. The experiment group consisted of security professionals working in industry in different positions, and within the experiment, the participants received the

information on a random basis. Therefore, randomisation was applied to some degree. The information provided in the experiment, especially in case C - where a security requirements description was provided - could have influenced the results. But cases A and B show at least that vulnerability identification errors occur; case C provides an indication that security requirements help to resolve errors, as vulnerability errors and also the total number of identified vulnerabilities decreased.

7.3. Future work

In this thesis it was demonstrated that the explicit evaluation of security requirements in the business process context can resolve vulnerability identification errors. The research contributions and limitations provide several points for improvement and future work, which is not unusual for research work. These are identified and outlined below.

The evaluation of security requirements in current approaches can improve the accuracy of vulnerability identification, as these approaches use techniques such as security testing, which only prove the presence of vulnerabilities - not their absence (Wang, 2005). One of the questions arising is at what stage of the assessment, and based on what information, the evaluation of an asset's security requirements can be performed. The vulnerability identification phase, as defined by NIST SP 800-30 (Stoneburner et al., 2002b), would be an appropriate point to perform a security requirement evaluation, as assets and possible threats are already identified. If no business process models are available for the evaluation, an intermediate model like the enterprise architecture of Innerhofer-Oberperfler and Breu (2006) could be used for modelling the information flow, business

context and dependencies between information assets. In principle, the evaluation could also be performed on single assets. However in that case, security requirements' dependencies - with regard to assets or processes - would be lost. Whether the joint usage of threat and security requirement evaluation in such an approach increases the result accuracy and can provide a statement of security – regarding the presence and absence of vulnerabilities - should be further explored. More work and verification is necessary to ascertain whether the absence of vulnerabilities can really be indicated by security requirements, and whether this statement holds.

In this research, tool support and modelling security requirements evaluation were not the focus. Automatising the evaluation - for example, by creating constructs in modelling languages like BPMN - would increase efficiency. BPMN extensions, like the work of Rodriguez et al. (2007), could be used to model security requirements. The modelling of process points (EP, PP or CC), security requirements and the corresponding evaluation results could be beneficial for the automatisation and visualisation of the assessment, as well as for security analysis. If process points – the current security implementation – and the security requirements are modelled, the evaluation procedure could be automatised and thus time saved. Furthermore, the visualisation of the vulnerabilities' impact on the output of the business process, or their effects on process activities could be supported. A first step with regard to automatisation is the Prolog program implementation for security objective assessments. Future work could focus on enhancing the rule base for security requirement and IT process evaluation, as well as on the usability and input options for the query interface. But one problem still remains: the current security implementation has to be expressed in the model

language and the security requirements properly defined by the security expert. Therefore, the procedure would still be a subjective process.

Haley et al. (2008) state that security objectives between stakeholders can be conflicting, but that they *should* be consistent. The verification of inconsistencies, conflicts and dependencies between security requirements, as well as between security goals, was not one of the aims of this research. With the elicitation of the information assets' security requirements, inconsistencies and dependencies between business processes for the same information asset can be identified, as only one set of security objectives and requirements is used for each asset. However, any conflicting security requirement definitions between information assets for business processes cannot be identified by the proposed approach. Furthermore, whether the security requirement satisfies the security objective of an information asset is currently not verified; satisfaction arguments could be used for this, as suggested by Haley et al.

Haley et al. define security requirements as "constraints on the functions of a system" (Haley et al., 2008, p. 136), while Firesmith describes "a detailed requirement that implements an overriding security policy" (Firesmith, 2003, p. 54). Tondel et al. (2008) recommend describing what should be achieved by the security requirements - not how it should be done. In this thesis, security requirements refine security objectives and describe what should be protected by a concrete security function implementation, in order that the asset is not harmed by any event. Non-adherence to these requirements would potentially cause harm to the organisation - defined as "risk" in this thesis. It would be interesting to further examine the negative impact aspect (harm to the asset) of our security

requirement risk definition, and how this should be reflected in the security requirement specification.

IT security processes ensure that systems operate securely and are well managed. Best practice IT security processes are proposed by security guidelines, like the baseline protection manual (BSI, 2008), or in IT service management best practices, such as ITIL (CCTA, 2007). Often vulnerabilities are caused by IT security processes that do not operate properly. In the proposed security requirements risk assessment approach, the definition and evaluation of IT security processes are not formalised; the security expert instead has to select and define these processes for the information asset and evaluate them by using best practice IT process standards. Process maturity and performance could be used as assessment criteria, as proposed by SSE CMM (Paulk et al., 1993). However, process maturity and performance evaluation causes additional assessment work and adds complexity to therrhe approach. Including process maturity in the assessment process is a long way off, and may not be accepted by security professionals. It would be interesting to see how the IT process selection and evaluation could be automated, and whether process maturity evaluation increases complexity or could, in fact, be made to be lightweight.

Appendix

A.1. Survey

i. Overall summary

The aim of the confirmatory and exploratory study, "Implementation of IT risk assessments and the use of security requirements in practice", is to find out which criteria in IT risk assessments are used, how they are used, to identify whether data such as process models and security requirements are available in practice, and whether data classification is used. The study is based on a survey conducted at an information security conference on February 25th, 2011. The survey was carried out before a presentation on security requirements and the participants had 30 minutes to answer the questionnaire. The study and the questionnaire were designed based on the work on a PhD thesis on IT risk assessments with business process models and security requirements. In the following, the main results of the study are presented.

Most companies perform IT risk assessments periodically with the focus being on systems or specific security issues. The standards and methods used for IT risk assessment are usually best-practice methods that specify which security measures have to be implemented - such as security processes, controls and security measures. The identification and assessment of an asset’s risk is mainly carried out using expert knowledge and system testing. Other methods or tools are rarely used. About 80 per cent of the participants use a repository in which data on assets (data, IT systems), security requirements and threats are documented. As part of a risk assessment, it is mainly the security controls of the audited assets

with vulnerabilities which are reviewed. Most participants agree that risks cannot be determined objectively and risk assessments are influenced by internal issues, such as cost savings or management attention, and external media.

As a driver for business process modelling, regulatory requirements and increase of productivity and efficiency were stated. In most companies, about 80 percent of critical processes are modelled and models are up-to-date. Risks, controls and security requirements are not modelled. At 90 percent of the participants' companies, objects such as IT systems, data or processes are classified according confidentiality, integrity and availability, and security requirements are documented. Security requirements are partly used in the assets' risk assessment and for identifying threats. In addition, 70 percent of the participants are convinced that risks can be identified more accurately and precisely with the evaluation of security requirements, and that the assessment of maturity and the performance of IT processes could lead to more consistent risk assessments. Most companies do not actively measure the security of data; however, they do use security requirements to evaluate data security.

The results of the risk assessment conducted by the participants in the study show that the more accurately risks are identified, the more information such as security requirements, process models, etc., are available. However, participants did have difficulties identifying risk accurately in complex situations. The risk assessment results also show that assumptions are made by the assessor if there is either no information or the information is not accurate. This directly impacts on the risk identification and the risk results. About 90 percent of the respondents rated the presentation of risk results based on the data involved, the business process and the infringed security requirement as more useful than the presentation of risks based on probabilities and consequences.

Future developments of the IT risk assessment process should aim to integrate risk results with the evaluation process into an enterprise-wide view on risk. Only with connection to the enterprise risk management, can a company-wide overall risk perspective be created; this is necessary for the fulfilment of regulatory requirements. But the integration of procedures and results into the security and compliance monitoring should also be pursued - not only for efficiency reasons, but also because of the harmonisation of assessments. Furthermore, research should try to expand the database within companies and also to objectify the evaluation process. Not only should data about assets, security requirements, controls and threats be available, but also data about incidents, impacts and incident scenarios, as well as the dependencies between assets, processes and incidents, in order to analyse and evaluate risks more accurately. Moreover, risk assessment procedures should use company-specific information, such as security requirements, for information assets that allow for identifying risks in the context of business operations. This would reduce assumptions and estimations of errors, as well as enforce the consideration of any company-specific requirements. Ideally, all risk assessment and monitoring activities in the company would make use of the same data.

ii. Objective of the survey

IT risk assessments are carried out to identify and assess risks and their impact on the company. Based on the risk assessment results, measures for protection are derived and the current risk situation evaluated. The identification of threats and the assessment of probabilities and impacts are difficult in practice, because reliable data is often not available and evaluations are based on expert knowledge. Current risk assessment methods are based on the ad-hoc identification of threats and vulnerabilities of single selected objects (assets) based

on security best practices. This procedure makes it difficult to identify security design vulnerabilities or implemented controls in operation, as the security needed is not verified.

The objective of the study was to examine the current practice of risk assessments - in particular the procedures and criteria used in risk assessments, the trust in risk assessment results, the evaluation of security controls, the usage of security requirements, and the availability of process models.

The results and findings from the study are used a as foundation for developing a risk assessment process based on business process models and security requirements as part of a PhD thesis.

iii. Survey design

The survey has three parts. Parts 1 and 2 consists of a questionnaire which should confirm the hypothesis and explore current practices. The questionnaire was developed as part of a PhD thesis literature review on IT risk assessment with business process models and security requirements. The questionnaire was verified in a test run, as to what extent are the questions understood and can the responses be evaluated. Part 3 is a quasi-experiment which should test whether participants are able to identify vulnerabilities more accurately with different sets of information. The design of the quasi-experiment was tested before in a trial run by an individual with the same background as the conference participants with regard to understandability, time required and the results generated.

a) Questionnaire

The questionnaire consists of the following three components:

‘Part 1 - IT Risk Assessment’ consists of questions about IT risk assessment; in particular, what criteria are used and how risk results are valued.

‘Part 2 - Business Process Models and Security Requirements’ consists of questions concerning the use of business process models, classification of data in enterprises and the use of security requirements in risk assessments.

‘Part 3 - Risk Assessment Example’ consists of a risk assessment task. The study participants had to carry out a risk assessment based on the information given.

b) Survey performance

In a lecture at an information security conference on February 25th, 2011, the participants were interviewed using a questionnaire regarding IT risk assessments and the application of security requirements. The survey took place in a closed room under supervision. The participants had approximately 30 minutes to answer the questionnaire. Interaction with other participants was not allowed and the survey instructor’s involvement was limited to answers on how to fill out the template. Out of the 55 participants of the meeting, 45 answered part 1 of the questionnaire and 46 answered part 2. Part 3 of the questionnaire was answered by 36 participants. Multiple answers were allowed for some questions.

iv. Survey results

a) IT risk assessments (Part 1)

a. How often per year do you conduct an IT risk assessment in your company and will you set any priorities?

33 percent of the participants perform risk assessments on an ad-hoc basis and 67 percent on a periodic basis.

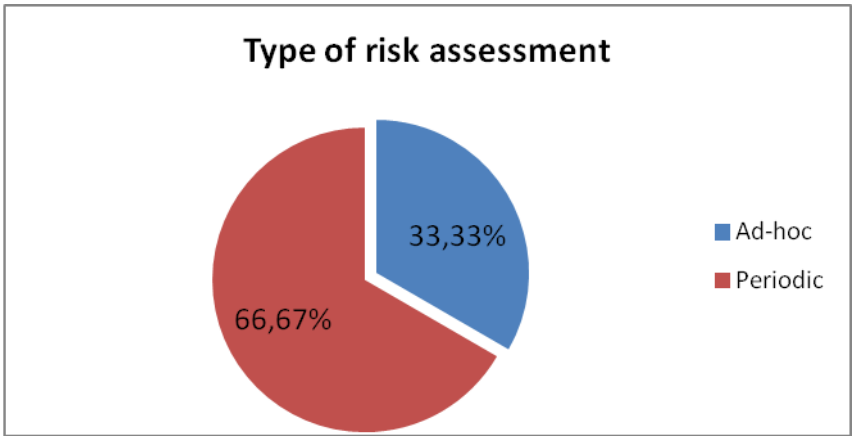


Figure A-1 Type of risk assessment

On average, each year 6 risk assessments are carried out. Usually these are done on specific security areas.

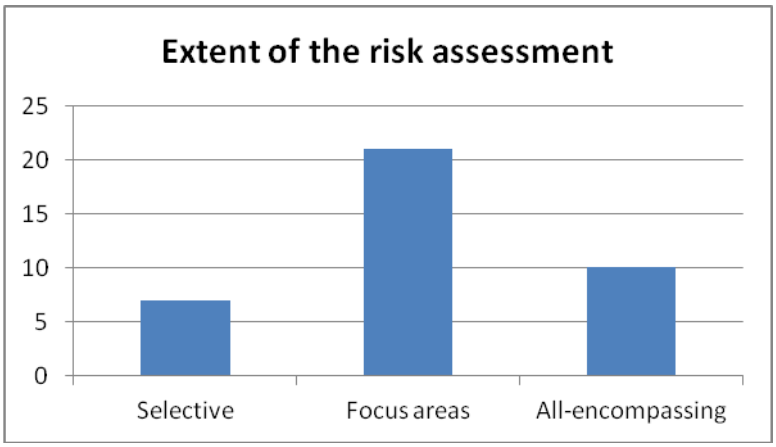


Figure A-2 Extent of risk assessment

b. What standards/ methods do you use for risk assessments?

Most participants use the ISO 27001/27005 standards, COBIT and ISF practices as a basis for risk assessment. It is noteworthy that security best practice standards are used that specify concrete security or control measures, and no risk assessment procedures, in a strict sense, are used, such as NIST 800-30 or Octave.

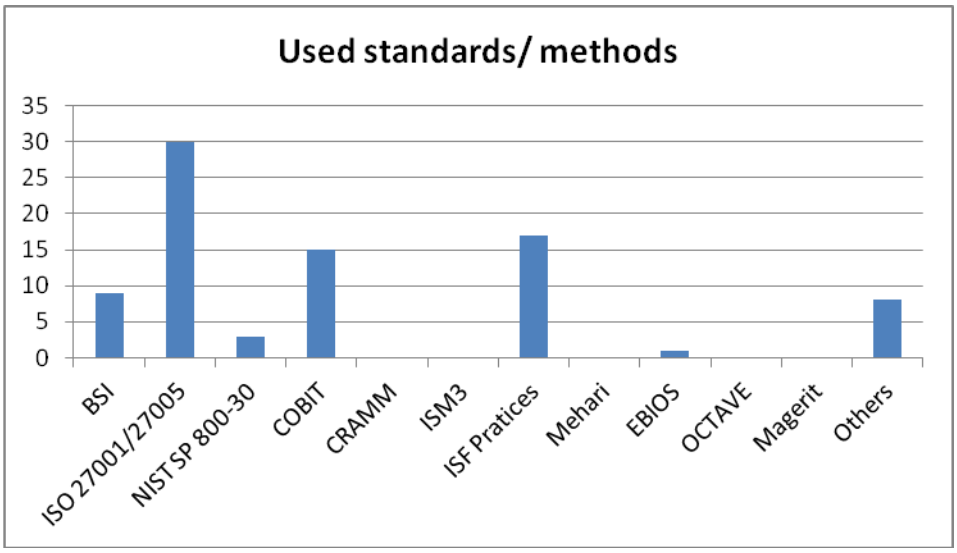


Figure A-3 Used standards/ method for risk assessments

c. Which of the following criteria do you use in the risk assessment?

Security controls, security requirements and frequencies are used by only some of the participants in the risk assessment.

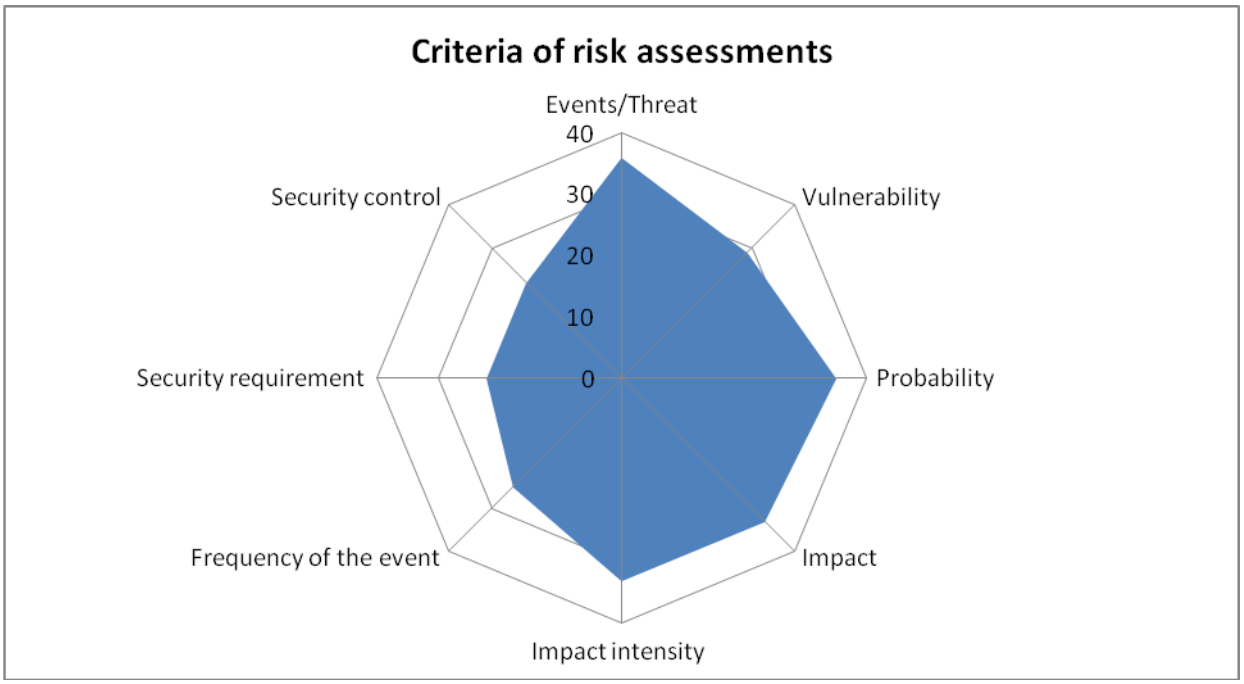


Figure A-4 Criteria's used in risk assessments

d. How do you determine or identify: events, vulnerabilities, probabilities, effects?

Events are mainly determined by using expert knowledge. Other tools such as publications and event databases are rarely used.

Weaknesses are mainly determined by means of expert knowledge, as well as system testing.

Probabilities are mainly determined by using expert knowledge and scenarios.

Effects of events are mainly determined by using expert knowledge and scenarios.

The identification of events, vulnerabilities, probabilities and impacts will be largely determined by expert knowledge. The result was as expected, but also shows the very high dependency on experts and their assessment of risks. Apart from system testing and scenarios other means for identification of events, vulnerabilities, probabilities and impacts are rarely used.

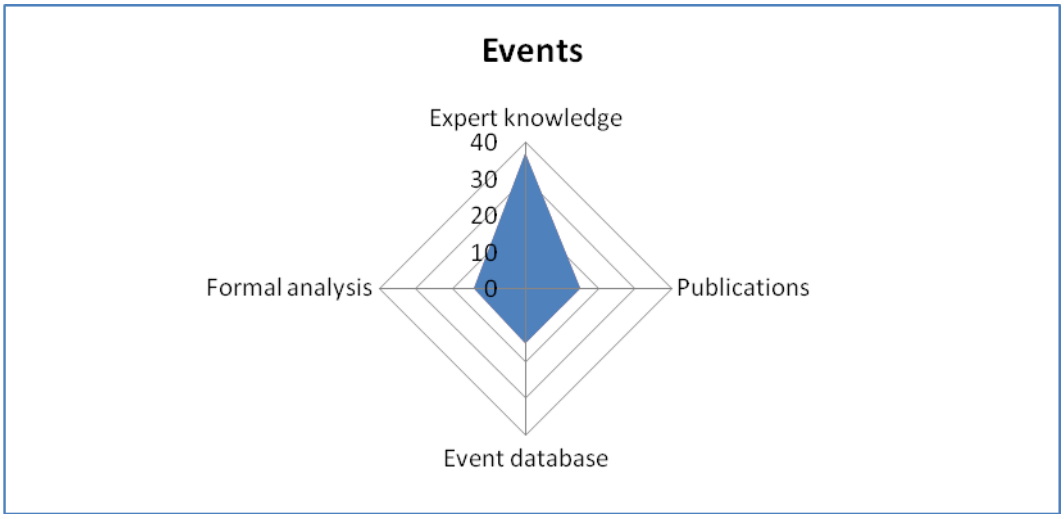


Figure A-5 Determination of events

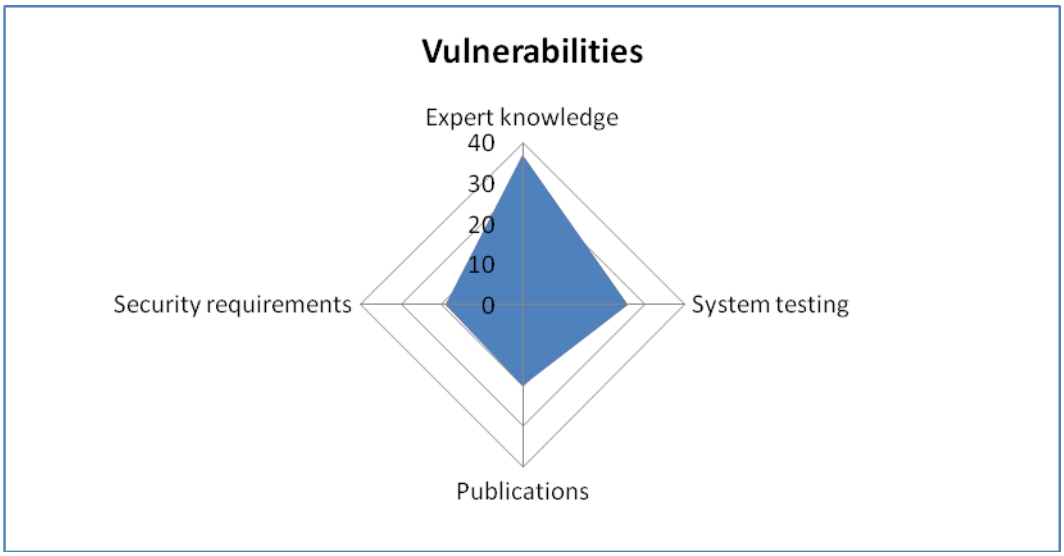


Figure A-6 Determination of vulnerabilities

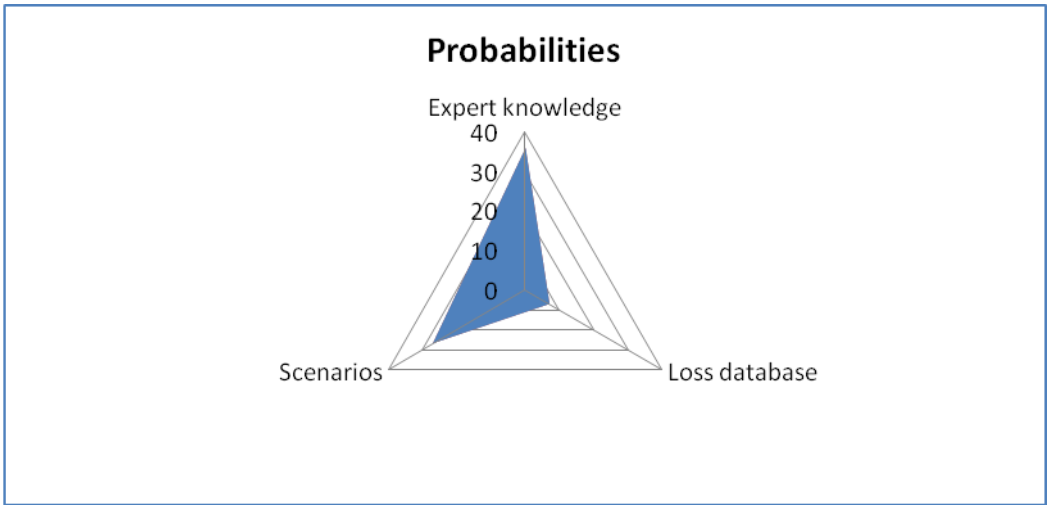


Figure A-7 Determination of probabilities

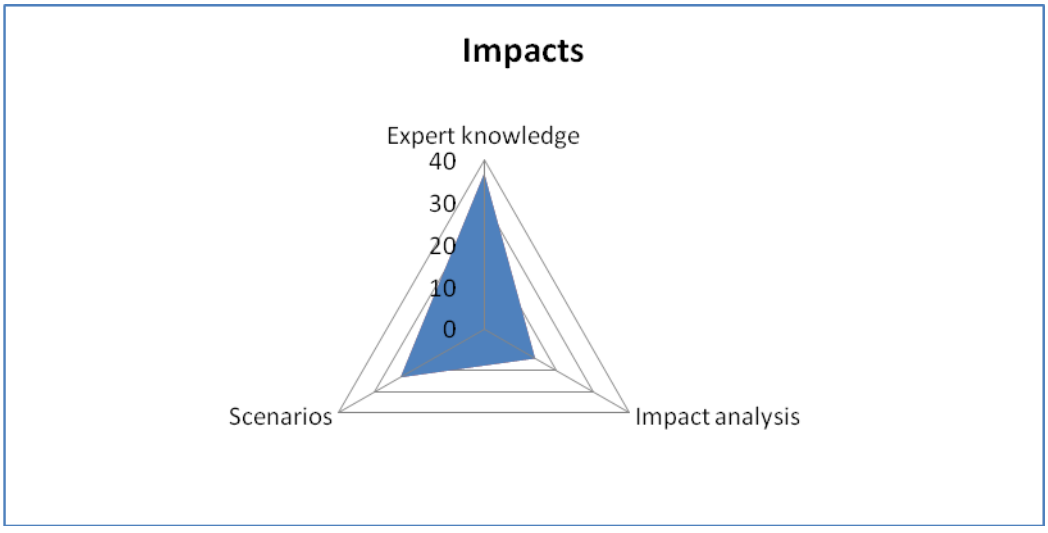


Figure A-8 Determination of impacts

e. Do you use a repository with the following objects for your risk assessment?

Approximately 80 percent of the participants use a repository which is used in the risk assessment. At most participants' companies, the evaluation objects (assets) and security controls / security concepts are stored in the repository. Security requirements, threats and impacts are often also stored in the repository. Potential losses or occurred ones are rarely documented.

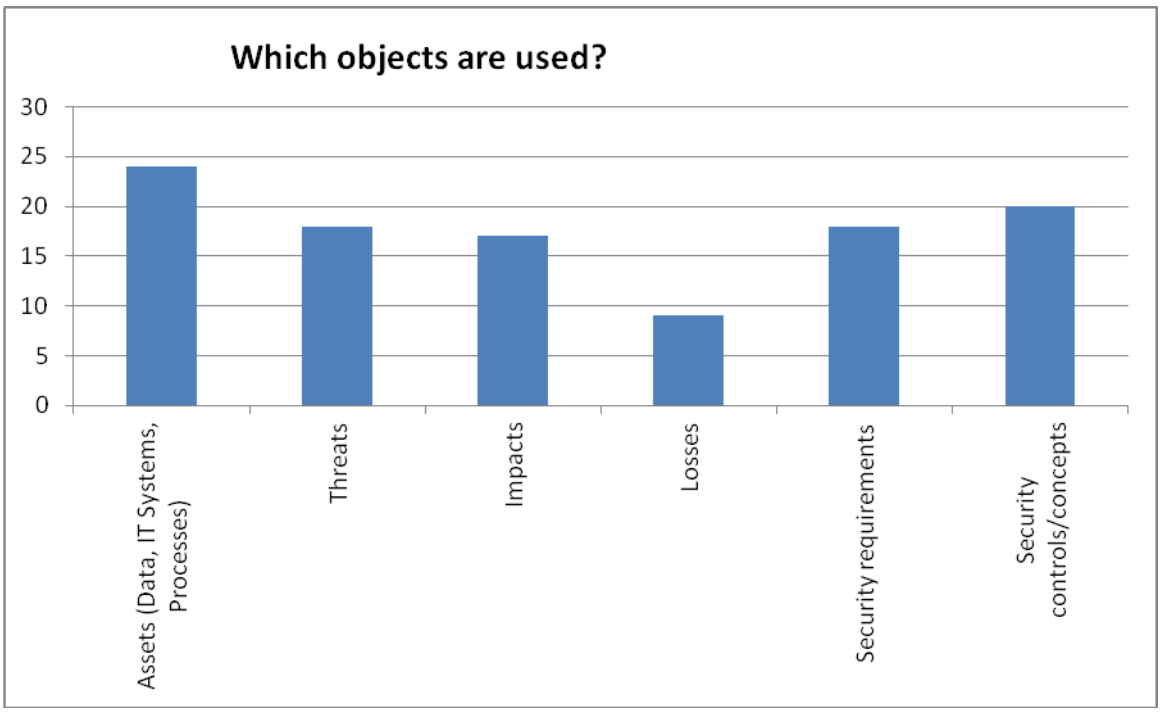


Figure A-9 Repository objects

f. Do you evaluate implemented security controls in the risk assessment?

Most of the participants do not evaluate all implemented security controls, nor do they evaluate security controls only for assets with vulnerabilities. Some of the participants evaluate controls for the evaluated assets and only a small part evaluated the security controls of all assets.

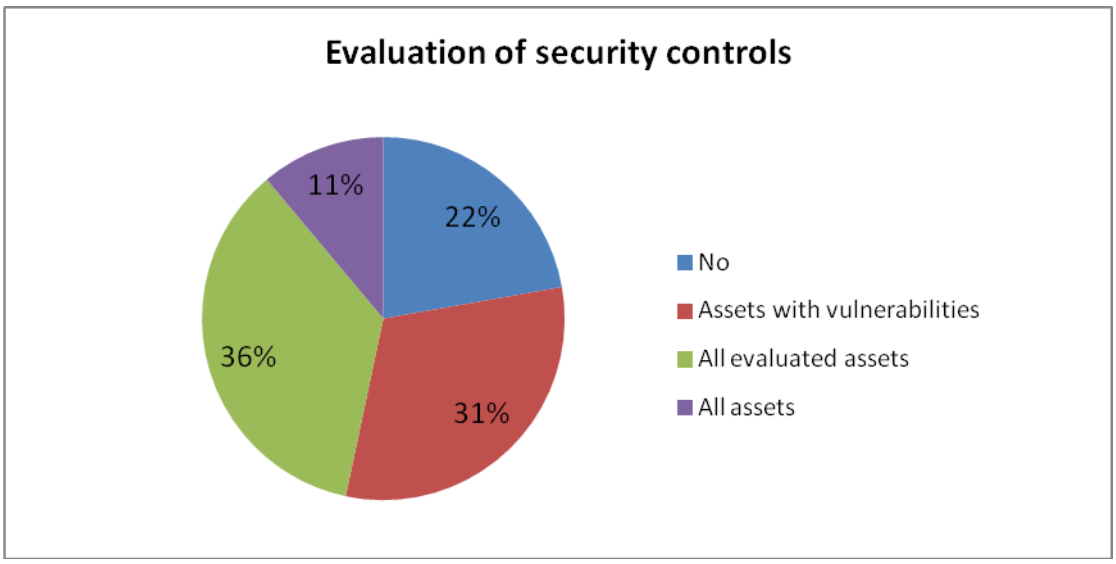


Figure A-10 Evaluation of security controls

g. *To what extent do you agree with the following statements?*

(1) Risks cannot be determined objectively, because of insufficient data on events, probabilities and consequences, as well as statistical data not being available.

Most participants agree that risks cannot be determined objectively. However, there is the view among the participants, that the risk results are verifiable and therefore not subjective (see (2)). This would mean that risk results are comprehensible, but the data basis used is not verifiable. But how should the risk result then be comprehensible? Furthermore, the participants felt that risk assessments are influenced by e.g. personal experience or media (see (3)). But this raises the question of how risk assessments are really verifiable, as the participants confirmed that there is a (subjective) assessment on the basis of negative experiences.

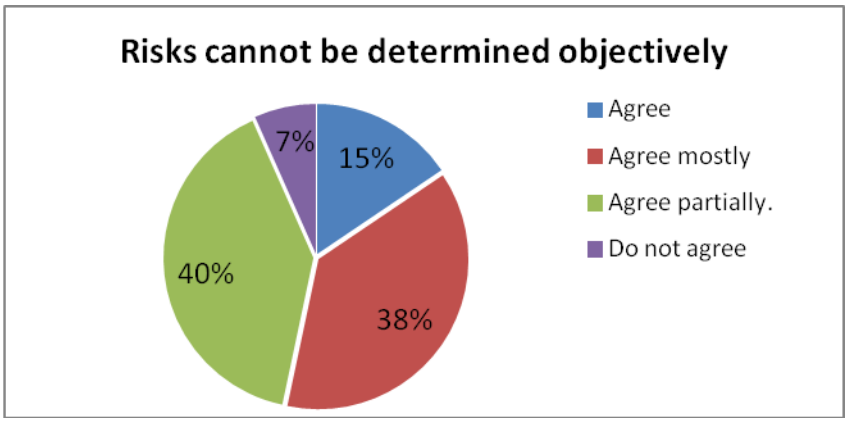


Figure A-11 Objectivity of risks

(2) Risk assessments are subjective estimates, which are difficult to verify.

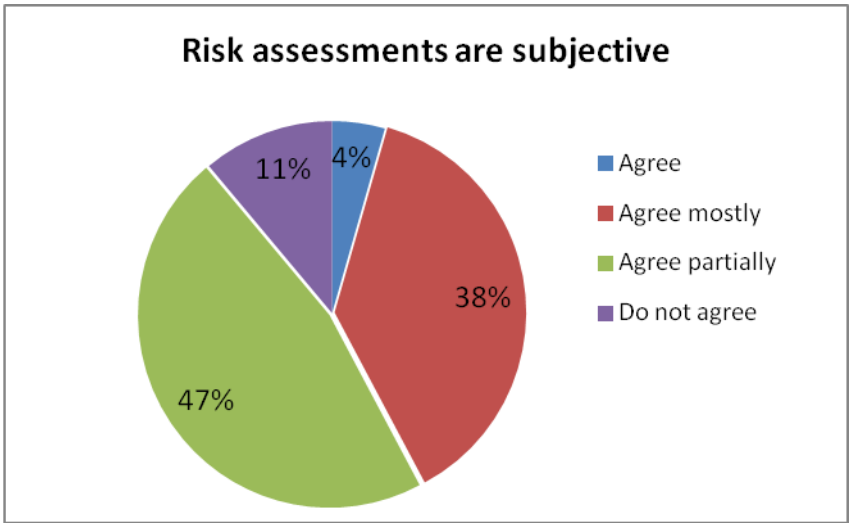


Figure A-12 Risk assessments are subjective

(3) Risk assessments (probabilities and consequences) of an assessor are influenced by personal experiences, media and business-specific circumstances

About 80 percent of respondents believe that risk assessments are influenced by personal experiences or media and therefore vulnerability identification error occur.

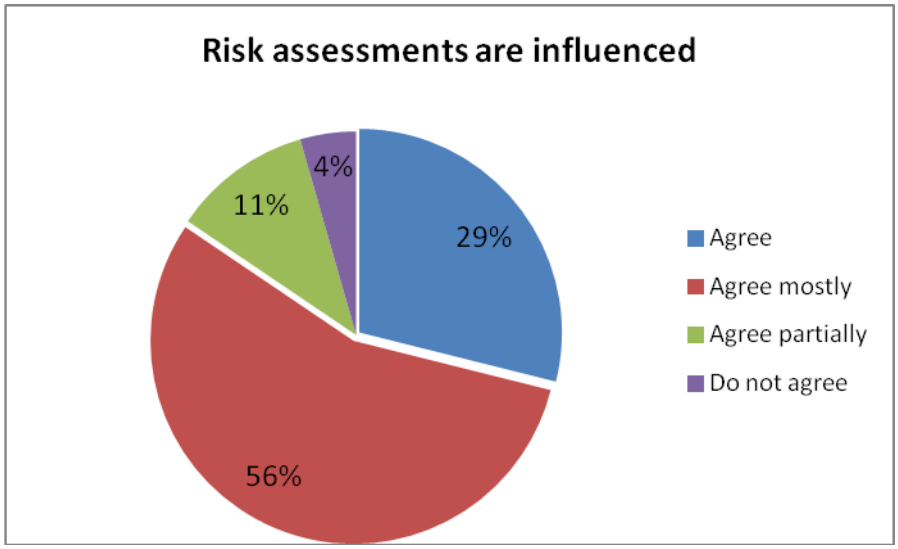


Figure A-13 Risk assessments are influenced

(4) Risks are usually assessed as low or medium; therefore high risks (H) are under-represented and low risks (N) are over-represented

High risks are not seen as under-represented and low risks are not seen as over-represented. This is interesting since it has been scientifically proven that some risk assessment procedures tend to classify risks mainly as medium or low. In a separate study carried out in a company it has been identified that low risks are over-represented compared with a normal distribution.

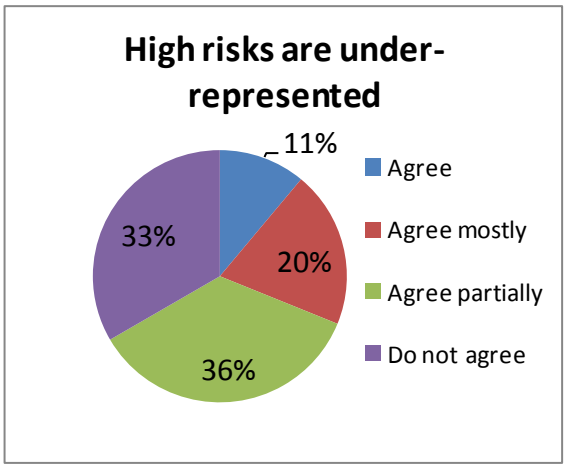


Figure A-14 High risks are under-represented

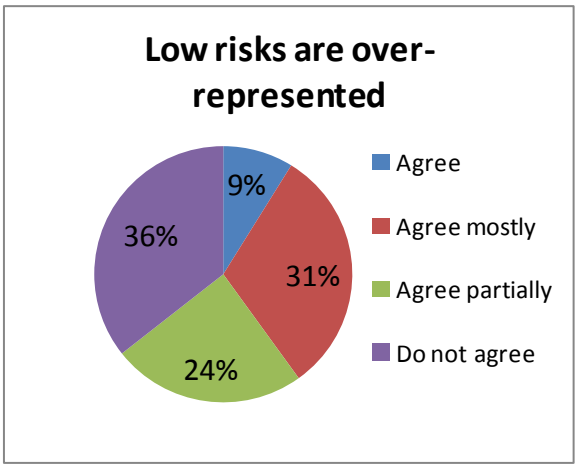


Figure A-15 Low risks are over-represented

(5) The implementation of security measures by the management is influenced by personal, departmental or company-wide cost objectives

The implementation of security measures is influenced up to 90 percent by the management and cost objectives.

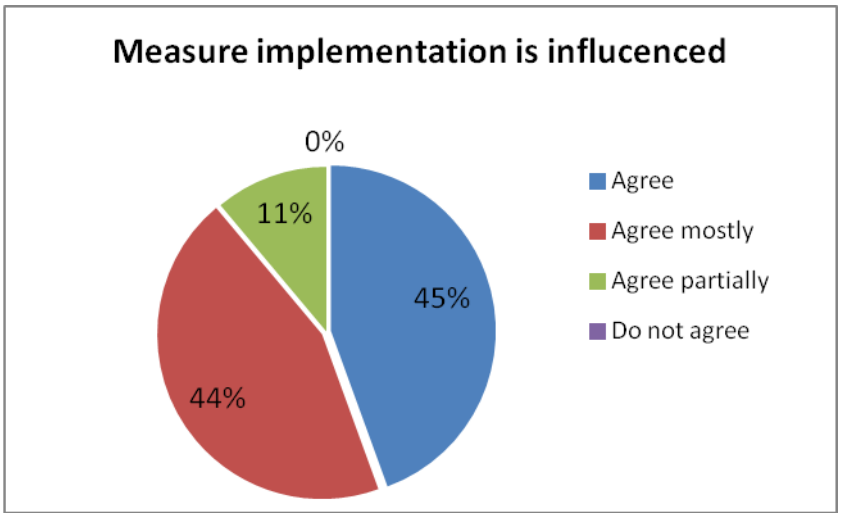


Figure A-16 Measure implementation

(6) Security policies are adjusted when risks are accepted by management

There is disagreement among the participants about whether security policies are adjusted when risks are accepted by the management. Security policies are only partially, adapted or may not be adapted at all.

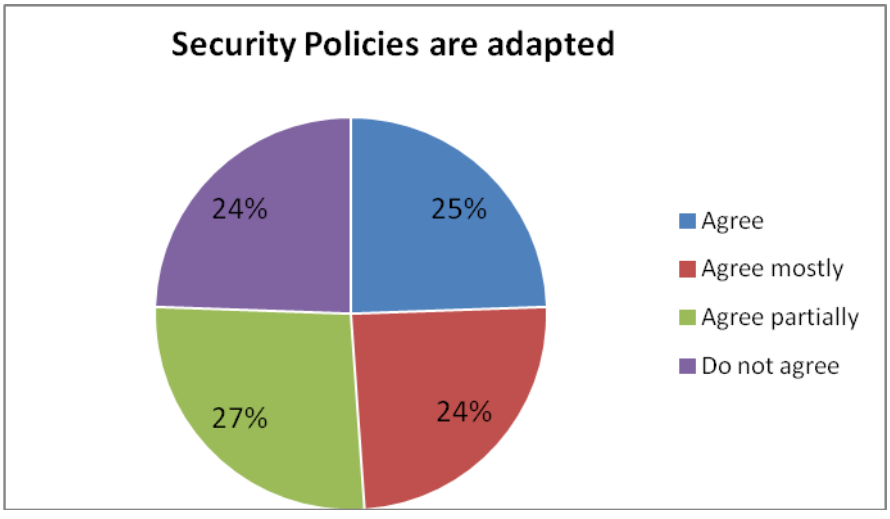


Figure A-17 Adaption of security policies

(7) Current risk assessment processes or methods (see question 4.2) are sufficient.

51 percent of the participants have the opinion that the existing risk assessment procedures are sufficient and 49 percent believe they are not. The following issues should be considered to improve current methods: risk management and compliance, objectivity of assessment procedures, dependencies between risks and assets, and the coverage of the assessment process.

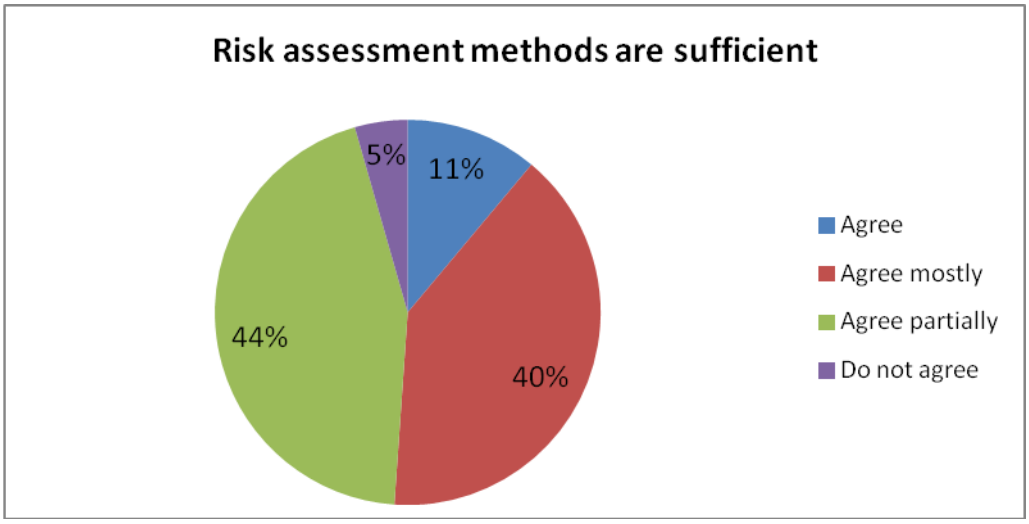


Figure A-18 Risk assessment methods

h. Summary - IT Risk Assessment (Survey Part 1)

Most companies perform IT risk assessments periodically with a focus on key assets or specific security areas. On average 6 assessments per year are carried out. The standards / methods used for risk assessments are usually best-practice methods that specify which concrete security measures such as security processes and security controls should be implemented. The most frequently mentioned methods were standards such as ISO27001, Cobit and ISF practices. Partly self-developed assessment procedures are used that are created from

existing best-practice standards. The identification and assessment of risks of assets is conducted primarily by expert knowledge. Partially system testing and scenarios are used. Other methods or tools such as publications, loss or event data play a relatively minor role in risk identification and assessment. Approximately 80 percent of the participants have a repository in which data on assets (data, IT systems), security requirements and threats are documented. In a risk assessment largely implemented controls at assets with vulnerabilities are evaluated. However, security controls implemented for all assets of the company or for assets assessed are not systematically checked.

Most participants agree that risks cannot be determined objectively; however, they believe that risk assessment results can be verified. In addition, the participants agreed that risk assessments are influenced either by the assessor and / or cost objectives in the company and vulnerability identification errors occur. To what extent security policies are adapted after the risk assessment, and the decisions made about risk, are very individual depending on the company. The participants have not confirmed that there might be a concentration of risks in specific ranges: e.g. a high number of low or medium evaluated risks or an insufficient number of high risks.

b) Business process models and security requirements (Part 2)

a. What do you see as a driver for the modelling of business processes?

As a driver for business process modelling regulatory requirements, increased productivity and efficiency are seen. Organisational design and organisational documentation play a relatively minor role.

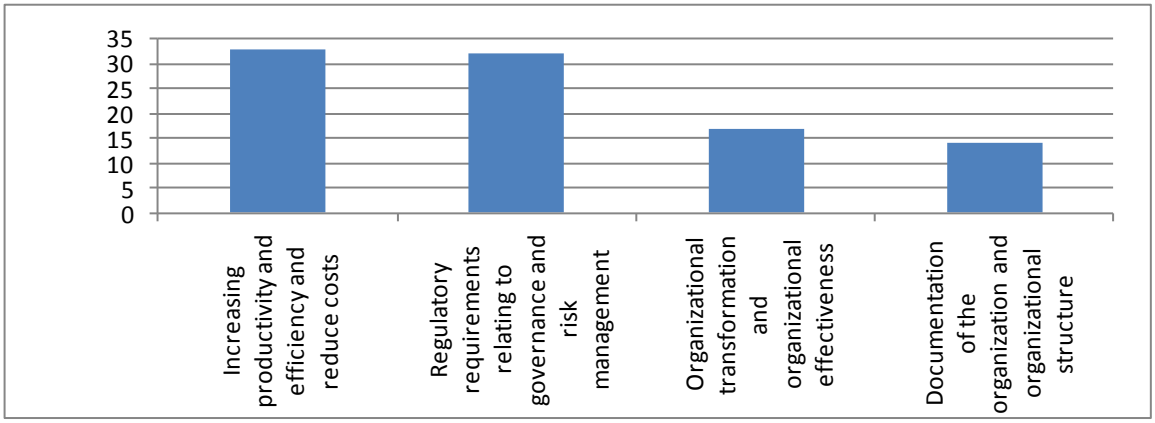


Figure A-19 Driver for business process modelling

b. Has your company (group or subsidiary) modelled business processes (1), are they up-to date (2) and for the most part are important / critical (3) processes available?

In most organisations of the participants critical or important processes are modelled and up-to date.

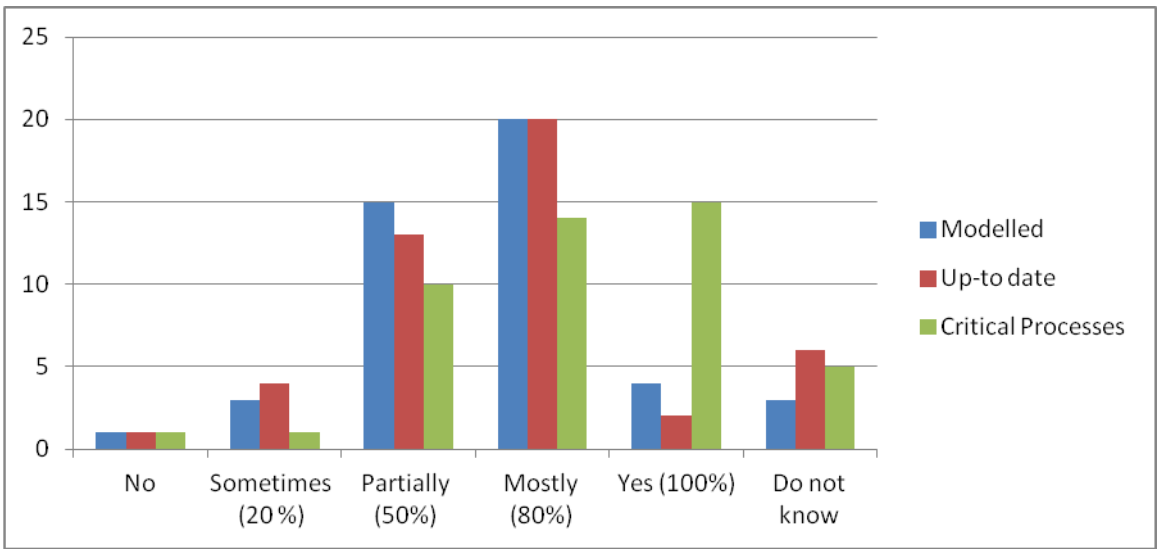


Figure A-20 Business process modelling

c. <u>What information is modelled in the business process models?</u>

Mostly actors / roles and IT systems are modelled in the business process model. Risks, controls and security requirements are usually not modelled.

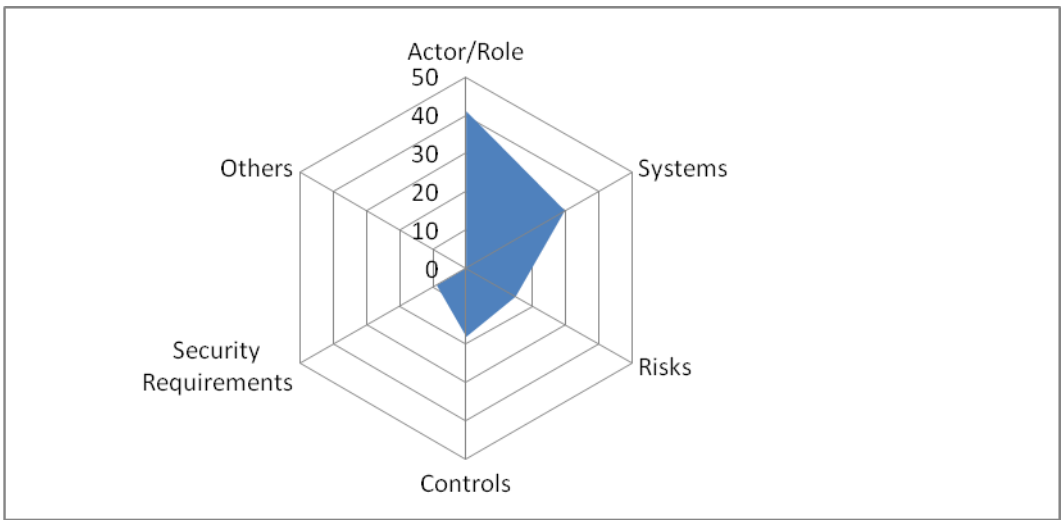


Figure A-21 Information in business process models

d. <u>Do you classify information objects company-wide according to confidentiality, integrity and availability?</u>

In 90 percent of the participants' information objects are classified by confidentiality, integrity and availability; mainly IT systems and data are classified.

e. *Do you have defined security risk limits as well as security requirements in your company?*

For 60 percent of the participants, limits for security risks and security requirements for systems and data are defined.

f. *For which information assets are security requirements defined at your company?*

Security requirements are mainly defined for IT systems, data and partly for processes.

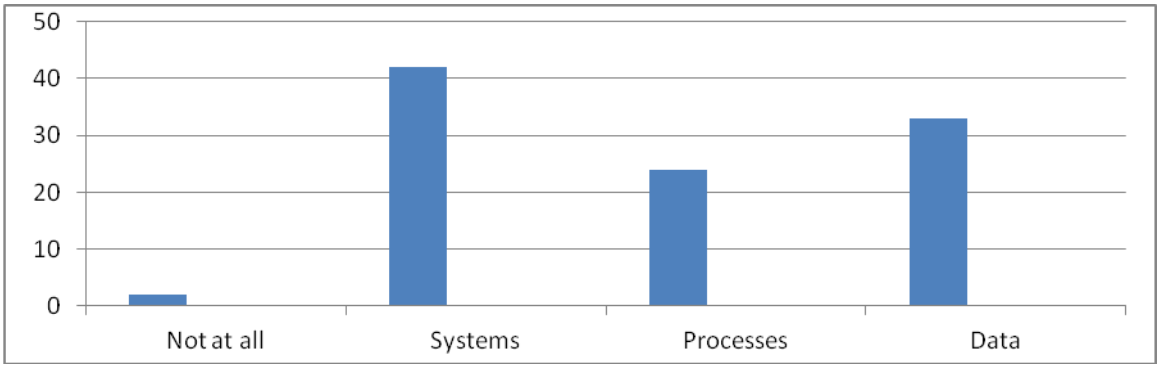


Figure A-22 Security requirements for objects (assets)

g. *How are security requirements documented in your company?*

Security requirements are usually documented either in a structured template or as free text.

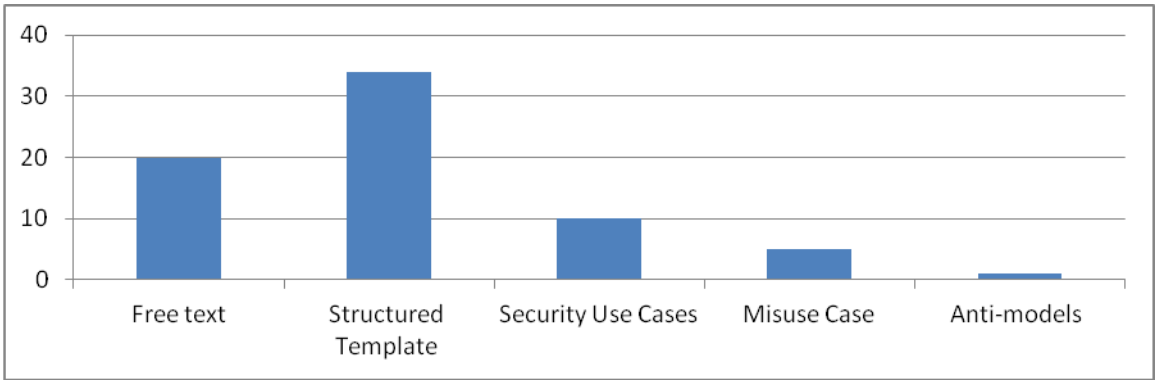


Figure A-23 Documentation of security requirements

h. Where are security requirements defined in your company?

Security requirements at most companies are defined in security policies and / or security standards, and / or Security Procedures / Guidelines.

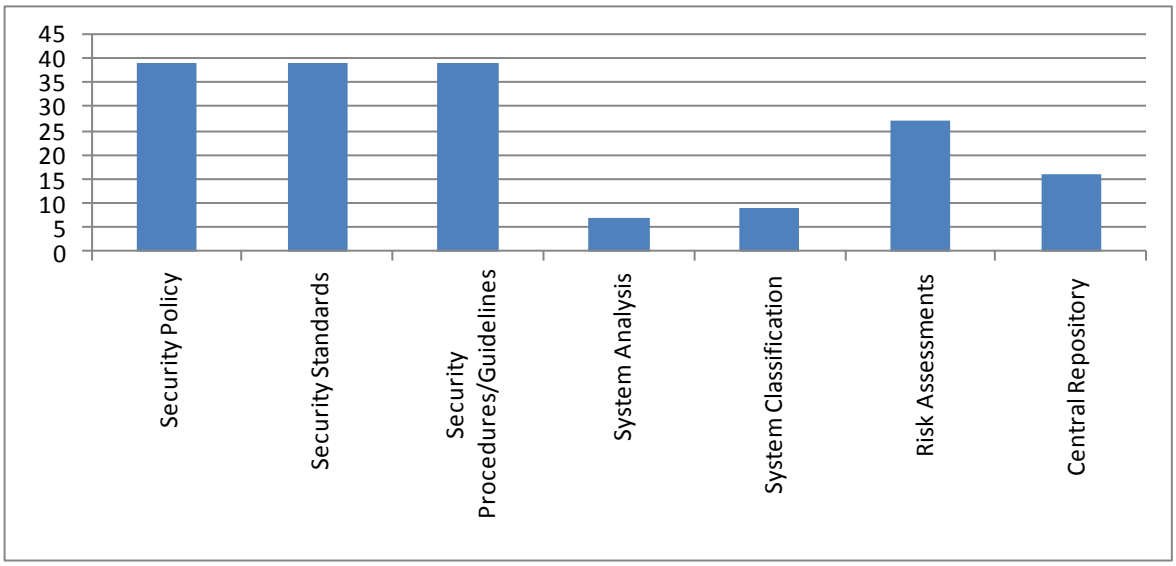


Figure A-24 Documentation of security requirements

i. Do you take advantage of security requirements in the risk assessment?

Security requirements are used for assets and / or for the identification of threats and / or the assessment of events.

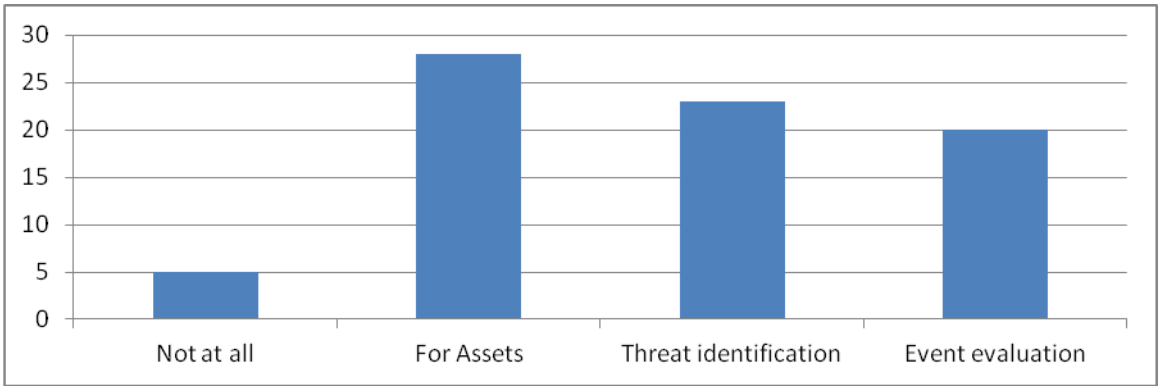


Figure A-25 Usage of security requirements

j. To what extent do you agree with the following statements?

(1) Security requirements are systematically (for threat identification and the assessment) considered in risk assessments. Risks could be determined to be more precise/accurate with a systematic evaluation of security requirements.

In most organisations of the participants (60 percent), security requirements are already taken into account in the risk assessment. In addition, 70 percent of the participants are convinced that risks can be determined more accurately and precisely with the evaluation of security requirements.

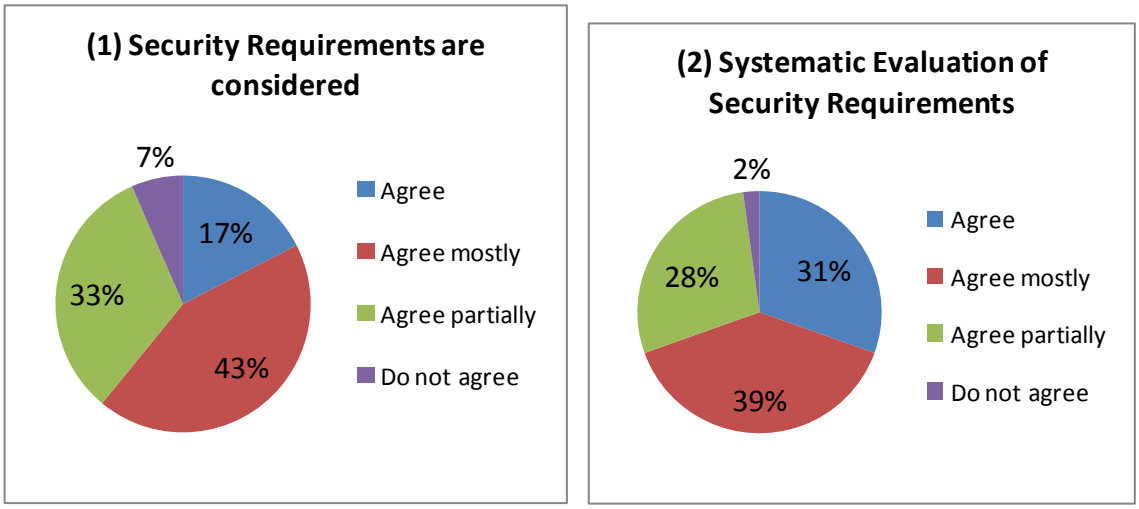


Figure A-26 Consideration of security requirements

(2) Risks can be identified and assessed only on the basis of security requirements.

Most participants do not believe that risks can only be identified and evaluated on the basis of security requirements.

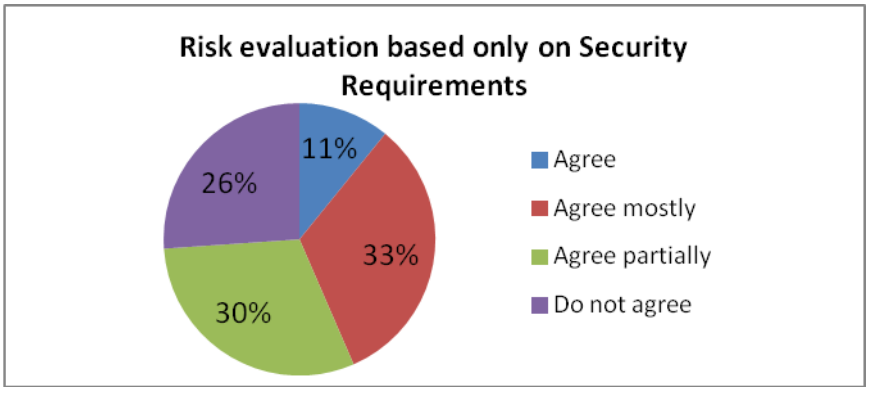


Figure A-27 Security requirements as basis for risk assessments

(3) The additional assessment of maturity (Mat) and Performance (Perf) of IT processes could lead to more stable (time-independent) risk assessment results.

The majority of participants confirmed that the assessment of performance and maturity of IT processes could lead to more consistent and time-independent risk assessment results.

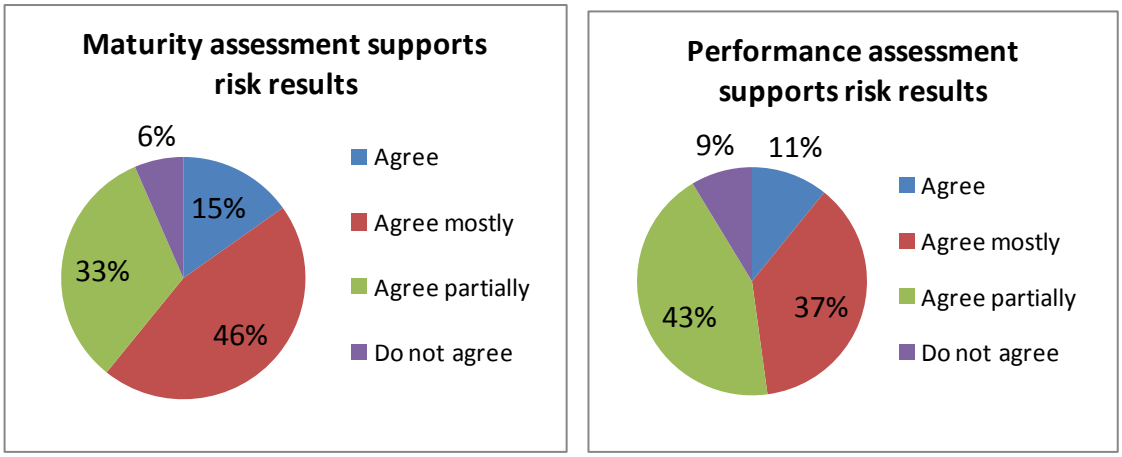


Figure A-28 Maturity und Performance in risk assessments

(4) Within our company we already systematically check information security by means of security requirements (SR)

Security requirements are used to determine risks. About half of the participants systematically evaluate information security with security requirements.

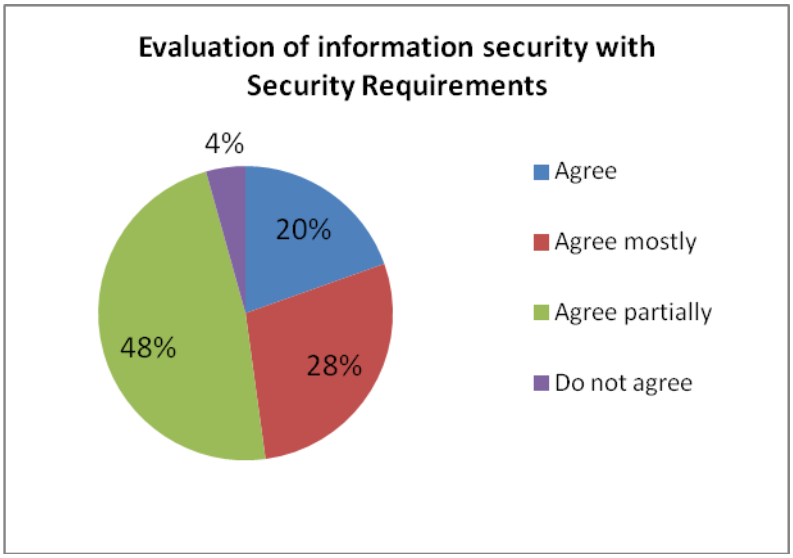


Figure A-29 Information security with security requirements

(5) Our company actively measures information security with security metrics.

Most companies do not actively measure information security.

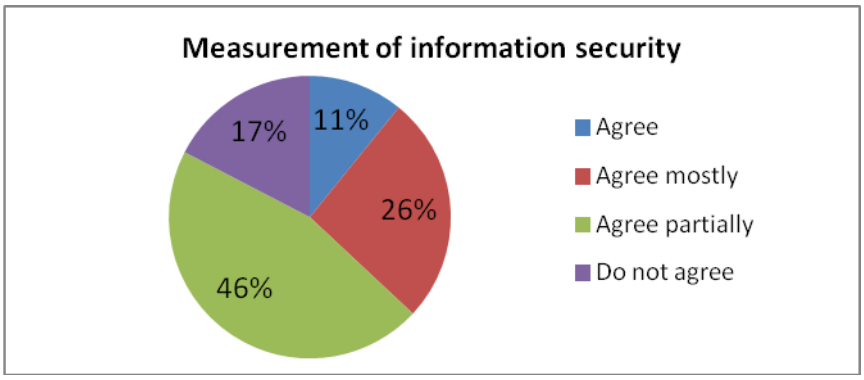


Figure A-30 Measurement of information security

(6) Which representation of risk is more useful for you?

The presentation of risks associated with the process, the data and the security requirement violated, are viewed by about 90 percent of respondents as very helpful (Representation 2 and 3).

Table A-1: Representation of risk results

Representation 1 (L=Low; M= Medium; H=High)			
Risk	**Probability (L/M/H)**	**Impact (L/M/H)**	**Risk assessment:**
Web server – Not encrypted data transmission	Low	Medium	Expert

Representation 2				
Process	**Risk**	**Data affected**	**Risk assessment:**	
Sales process	Web server – Not encrypted data transmission	Customer data	Security requirement infringed	
Representation 3 (SR=Security requirement)				
Process	**Risk**	**Data affected**	**Risk assessment:**	**SR + Level (1-3)**
Sales process	Web server – Not encrypted data transmission	Customer data	Security requirement V2 infringed	Confidential (V 2) Integrity (I 1)

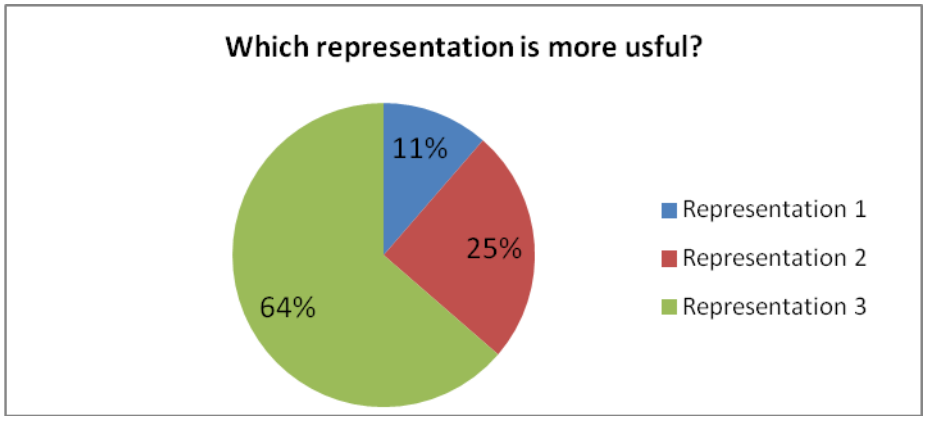


Figure A-31 Representation of risk results

k. Summary – Business Process Models and Security Requirements (Part 2)

The participants of the study see as a driver for business process modelling regulatory requirements and the increase in productivity as well as efficiency reasons. Organisational design and organisational documentation play a relatively minor role. In most organisations critical and important processes of the company are modelled and these processes are up-to-date. Usually actors / roles and IT systems are modelled in business processes. Risks, controls and security requirements are usually not modelled.

For 90 percent of the participants, information objects like IT systems, processes or data are classified according to confidentiality, integrity and availability. Mainly IT systems and data are classified, and for these security requirements are defined. Security requirements are documented either in a structured template, or as free text. Other forms of documentation for security requirements are not being

used. Security requirements are described in security policies and / or security standards and / or Security Procedures / Guidelines, and are used in risk assessments for identification of threats.

60 percent of the participants consider security requirements in the risk assessment. To what extent and at which risk assessment activity security requirements are used could not be determined. In addition, 70 percent of the participants are convinced that risks can be determined more accurately and precisely with the evaluation of security requirements. The presentation of a risk not only by the event, the likelihood and impact, but with the security requirements, the processes and data involved is seen as very helpful by approximately 90 percent of the participants.

The majority of participants confirmed that the assessment of performance and maturity of IT processes could lead to more consistent and time-independent risk assessment results. However, most companies do not actively measure information security, but use security requirements to verify information security.

c) Risk assessment by hand of a example (Part 3)

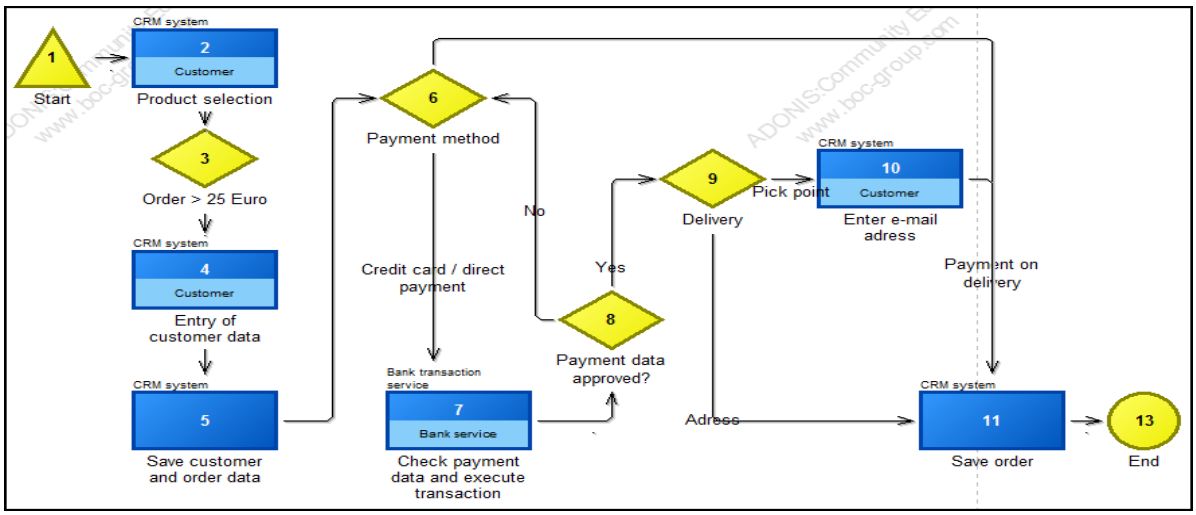
In this study, the participants had to carry out a risk assessment on a real world example. For this purpose, three different samples (A, B, C) were distributed among the participants. Examples A, B and C contain different amounts of information for the risk assessment. In example A (33% of all survey forms) a risk situation description was provided, in example C (33% of all survey forms) the risk situation description in addition to a business process model was provided and in example B (33% of all survey forms) the risk situation description along with security requirements and a business process model was provided.

The following information was provided in the examples:

Risk situation description:

A company sells all their goods through an online shop. Approximately 1000 orders per day are processed and only orders that are higher than € 25 are processed and stored in an online CRM system. If the customer wants to pay by credit card or by bank transfer, the payment data is forwarded to a bank which processes the payment transaction. The online shop is important for the company, as all sales are generated through the online portal. In a security analysis it was found that via the input fields in the online shop (CRM system) database content can be changed. In addition, customer data and payment data transmitted are not encrypted. All employees of the ordering process have read access to order data in the CRM system. The CRM system was not available in the last 10 days, on two occasions for 1 hour, due to a system failure caused by maintenance work.

Business Process model "Sales":



Security requirements description:

The business process "sales" is classified as critical for the operation of the company. For all customer- order- and payment data, confidentiality and integrity of the data must be ensured and IT systems should not exceed 15 minutes per day unavailability. In the business process "invoice" it was specified that only employees of accounting department may view all order data. Saved transactions (orders) in the sales process are to be authorised after saving the order, by a member of the sales process and are then to be transmitted to the “invoice” process.

In the following the assessment results for the examples A, B, C, of the participants are described. The evaluations per sample were carried out as follows:

Average number of risks identified: Number of identified risks of the participants divided by the number of evaluable results.

Reviews: Total number of rated risk as H, M, L, compared to all identified risks of the participants.

Risks: The risks identified by the participants were assigned to pre-defined risks (risk 1 - 5), which were described in the examples, or, if this was not possible, as other risks (Risk 6) declared but only one per participant. Then the total number of each risk (risk 1-5) and the percentage was determined.

a. Example A

For example A, we got back 17 of the 20 questionnaires distributed, of which 12 were evaluable. Example A consisted of the risk situation description, a textual description of the online sales process with a description of potential security vulnerabilities in the process.

Table A-2: Overview of identified risks in example A

Average number of identified risks		3,5	
Assessment	**Probability**	**Impact**	
High	23	29	
Medium	14	12	
Low	5	1	
Risks		**Number**	**Percentage**
1. Not authorised changes in the database (in example A, B and C)		12	100%
2. Unencrypted transmission of costumer and payment data in example A, B and C)		8	67%
3. Read access to order data (only in example B)		1	8%
4. Non-availability of the system (only in example B)		12	100%
5. Authorisation of an order (only in example B)		0	0%
6. Other risks (identified of the participants)		9	75%

In Example A, the majority of the identified risks were rated as high, which means the likelihood and impact of the risks was assessed as high. Only a very small portion of the risks have been rated as low. Most of the risks identified by the participants could be assigned to the security category availability; this is also reflected in the identified risks. The risks identified by the participants were

basically correct, except for the availability risk. There was indeed a statement in the example that the CRM system was not available for 2 hours in 10 days, but no evidence was provided showing that this really represents a risk for the company. In addition, three quarters of the participants had identified additional risks.

b. Example B

For Example B, we got back 17 of the 20 questionnaires distributed, of which 11 were evaluable.

Example B consisted of the risk situation description, a textual description of the online sales process with a description of potential security vulnerabilities in the process, the associated process model and the description of the security requirements.

Table A-3: Overview of identified risks in example B

Average number of identified risks	3,82	
Acceptable Risk	**No**	**Yes**
	37	5
Risks	**Number**	**Percentage**
1. Not authorised changes in the database (in example A, B and C)	8	73%
2. Unencrypted transmission of costumer and payment data in example A, B and C)	10	91%
3. Read access to order data (only in example B)	5	45%
4. Non-availability of the system (only in example B)	11	100%
5. Authorisation of an order (only in example B)	2	18%
6. Other risks (identified of the participants)	6	55%

The risks were identified fairly accurately by the participants. However, the participants had difficulty identifying correctly the risks that were associated with the design of the sales process (especially risk 5). The identified risks were almost all classified as non-acceptable risks, which was correct. Most of the identified

risks of the participants could be assigned to the security category confidentiality; this is also reflected in the identified risks.

c. Example C

For Example C, we got back 13 of the 15 questionnaires distributed, of which 13 were evaluable. Example C consisted of the risk situation description, a textual description of the online sales process with a description of potential security vulnerabilities in the process as well as the sales process model. The difference to example A was that the process model was available to the participants.

Table A-4: Overview of identified risks in example C

Average number of identified risks		3,46	
Assessment	**Probability**	**Impact**	
High	22	27	
Medium	14	15	
Low	9	3	
Risks		**Number**	**Percentage**
1. Not authorised changes in the database (in example A, B and C)		13	100%
2. Unencrypted transmission of costumer and payment data in example A, B and C)		11	85%
3. Read access to order data (only in example B)		0	0%
4. Non-availability of the system (only in example B)		11	85%
5. Authorisation of an order (only in example B)		0	0%
6. Other risks (identified of the participants)		10	77%

In Example C, most of the identified risks were rated as high; this means that the likelihood and impact of risks have been assessed as high. The identified risks of the participants were relatively equally distributed to the assigned security categories availability, integrity and confidentiality; this is also reflected in the identified risks. The risks were identified correctly with the exception of the availability principle. There was indeed a statement in the example that the CRM system was unavailable for 2 hours in 10 days, but no evidence was provided

showing that this really represents a risk for the company. Remarkable in comparison to Example A, which differs only by the additional process model, is that the risks number 2 and 4 were evaluated differently. In this example the process model has helped the participants to evaluate risks differently due to the visualisation of the process sequence.

d. Summary – Risk assessments by hand of an example (Part 3)

The average number of identified risks is roughly equal in the examples A, B, C. On average, in Examples A and C too many risks are identified and in Example B too few risks in relation to the pre-defined risks (risks 1 to 5). In the examples A and C, as an additional risk, the availability of the CRM system was mostly identified, probably based on the statement that the order process is important for the company, but without having a concrete statement on the criticality of availability. This shows that information is interpreted and assumptions made affecting the identification of significant risks and the correctness of the risk result. I.e. if more information about a risk is available, such as security requirements, the better the risk assessment results. One can observe this by the decreased additional risks identified in example B in contrast to examples A and C. It is also noteworthy that in all examples additional risks were identified in addition to the predefined risks. The number of additional risks identified decreases when more accurate information such as security requirements is available.

In Example B only a small number of participants managed to identify risks correctly that were linked to the design of the ordering process (risk 3 and 5). Certainly the abundance of information and the limited time influenced risk identification negatively. But in principle, this shows that if a lot of complex issues and information needs to be combined, the probability drops of identifying the risks correctly. However, it is important to emphasise that the correctness of the results

is significantly better than if less information is available. In current risk assessments single assets are assessed to reduce complexity, which in turn leads to the problem that associated risks are not identified correctly.

It is also interesting that in examples A and C, the classification of risks based on the security categories shows that the focus in example A is on the availability of data, whereas in example C the focus is on integrity. In comparison with example C the process model has contributed in that the integrity of the data was evaluated as more risky by the participants. The participants perceived the risks described in the example differently due to the visualisation of the process flow.

d) Discussion of results

The objective of the study was to collect information about IT risk assessments and the use of security requirements in practice, what, and how criteria and objects in IT risk assessments are used, as well to confirm that data such as process models, security requirements and data classification are available in practice and are used systematically. The aim was to investigate the following hypotheses from the perspective of security specialists in the field, and to what extent these hypotheses can be confirmed or denied. The confirmation or rejection of these hypotheses are used as the basis for the creation of a new risk assessment procedure based on business process models and security requirements.

Hypothesis 1: Risk assessment procedures are considered inadequate by security experts due to the subjectivity of results, insufficient data for assessments, the accumulation of risk, lack of systematics (only expert ratings), and inadequate consideration of frequencies.

Risk assessment procedures are considered in practice as procedures with shortcomings, but not completely rejected because of these deficiencies. It was reported by the participants that risks cannot be determined objectively and and vulnerability identification error occur, because of insufficient data. However, risk assessments are not considered as subjective by the participants even when assessments are influenced by external events. The accumulation of risk results e.g. of medium or high risk, was not identified as a problem or recognised as such in practice. The frequency of events is often not considered in risk assessments. Of the participants, improvement is seen in assessment procedures, particularly in the integration and combination of compliance and risk management and the efficiency of the assessment process. The existing assessment procedures are largely considered to be adequate by the participants.

Hypothesis 2: All security controls are reviewed in risk assessments based on security requirements.

The study reflects a mixed picture. Security controls are only partially evaluated, and only for assets with weaknesses. Several of the participants evaluated security controls for assets which are assessed in the context of risk assessment. A systematic assessment of security controls for all assets is not conducted.

Hypothesis 3: Business process models are available and up to date in practice.

The study has confirmed that business process models for critical and important processes of an enterprise are available and up-to-date. It is mainly actors, activities and IT systems which are modelled in the business process models. Risks, security controls and security requirements are not modelled. As a driver for

business process modelling, efficiency gains and cost reduction as well as regulatory requirements are seen by the participants.

Hypothesis 4: Security requirements are in part considered in the risk assessment, but not systematically used for the assessment of risks.

Security requirements are defined for IT systems and data and are usually described in the relevant security policies / guidelines. Security requirements are usually considered in risk assessments. To what extent security requirements are being systematically used in risk assessment, could not be verified. However, due to the fact that best practice methods are used and study participants have often not mentioned security controls and security requirements as criteria in risk assessment, it is unlikely that security requirements are used systematically.

Hypothesis 5: Security requirements are used in risk assessments, are defined for assets and used to measure risks.

Security requirements are used in the risk assessment for assets (IT systems and data) and the identification of threats as well as for assets defined. There is no active measurement of risk, but security requirements are used to verify data security.

Hypothesis 6: Data is classified throughout the company.

For 90 percent of the participants, companies' IT systems and / or data are classified according confidentiality, integrity and availability. Data classification is considered in the description of security requirements and the data classification is available in risk assessments.

Hypothesis 7: The assessment of risks with security requirements leads to better risk results, i.e. risks can be determined more correctly.

The risk assessment task performed by the participants shows that risks are identified more correctly, if more information such as security requirements is available. However, the participants had problems identifying risks correctly in a complex environment. It was also evident that within risk assessment assumptions are made, if there is either no information, or not precise information, which has a direct impact on the risk identification and result. The presentation of the risk assessment results based on the data involved, the process and violated security requirements was rated as more helpful than a presentation with probability and impact only. These results suggests that security requirements, and process data should be used more in the evaluation proceeding.

e) Conclusion

IT risk assessment procedures are considered by the participants of the study - i.e., IT security experts from industry - as approaches with shortcomings and weaknesses. Risk results and the risk assessment process are viewed as subjective; they can be influenced by various external issues such as risk awareness, cost targets or public media. In addition, existing risk assessment methods should be better aligned with enterprise risk and compliance management activities, and the effectiveness and efficiency of methods should be increased.

In the focus of future developments and improvements to risk assessment procedures should be the integration of risk results with the assessment process, in the form of an enterprise-wide risk assessment. Moreover, the integration of risk results into enterprise risk management should be enforced as well as the evaluation of all operational risks in all divisions, including IT systems, IT

processes and data. Only with the integration of decentralised risk assessments in the enterprise risk can management take an enterprise-wide view of total risk - necessary for the fulfilment of regulatory requirements. Furthermore, the existing database of risks and assets should be expanded to objectify the evaluation process, as well as to obtain risk results that can be objectively verifiable and are not only based on expert opinions. Not only should assets, security requirements, security controls and threat data be available, but so should data about incidents, damage potentials and scenarios, as well as about dependencies between assets, processes and incidents. This would enable managers to analyse and assess risks more accurately and precisely.

It is positive for the future development of risk assessment procedures that in the majority of companies, data such as business process models, security requirements and an asset repository may become available. This means that these data could then be used for risk analysis and assessment and be further enriched. Moreover, automated risk analysis and assessment procedures could be developed.

Security monitoring and security measurement is, in most companies, not very pronounced. Under these terms, the current and ongoing review of the security of information assets is understood. The existing risk analysis data in the company could serve as a basis for continuous monitoring; however, these data must be enriched and reliable methods should be developed for continuous security monitoring and measurement. In the field of compliance monitoring, there are already some initiatives in science and research dealing with this topic: business processes are used as a basis for verifying compliance with external regulations; agents are used to evaluate IT systems to ensure compliance with security policies, etc. It also applies to this topic that there should be a close link between

risk analysis and security and compliance monitoring - ideally using the same databases.

The risk assessment example in the study shows that risks are identified more correctly if more information, such as security requirements, is available. However, participants had problems identifying risks correctly in a complex environment. On the one hand, one needs more information in the risk analysis to identify risk correctly; on the other hand, this information should not increase complexity. Methods or tools for the presentation and analysis of information in complex environments in the context of risk analysis and assessment should be developed to make the assessment more efficient and accurate. Moreover, risk assessment procedures should use business context-dependent information for precise identification of risks, in order to reduce estimation errors, to eliminate assumptions and to reflect company-specific requirements.

A.2. The approach in UML

In this section, the security requirements risk assessment approach of section 5.2 is described in the Unified Modelling Language (UML) to demonstrate that the approach can be structured and formalised in a modelling language. The input of the program is business process models; as a result, the business process, information asset and the vulnerability are displayed. The approach's activities are presented within a UML activity diagram. Activity diagrams can describe procedural logic, business processes, workflows and can be compared to flowcharts, representing the steps as boxes, and their order using arrows.

Figure A-32 shows the approach's procedure as an UML activity diagram. Partitions are used to indicate the various phases. Within each partition, the activities and objects represent the approach steps and information. An object

represents information that is created, used or changed by the activities. An activity is a task performed by an actor or system that may use an object. Input and output objects, which can be attached to activities, are used to indicate that the activity needs information (input) to perform the task, or that the activity creates information (output) to be handed over to the next activity. Joins are used to distribute information to several activities, but do not necessarily indicate a parallel activity. Forks are used to merge information as inputs for an activity. An arrow indicates the flow between activities, or a sequence. Decisions are used to branch the flow, e.g. to restart or skip activities.

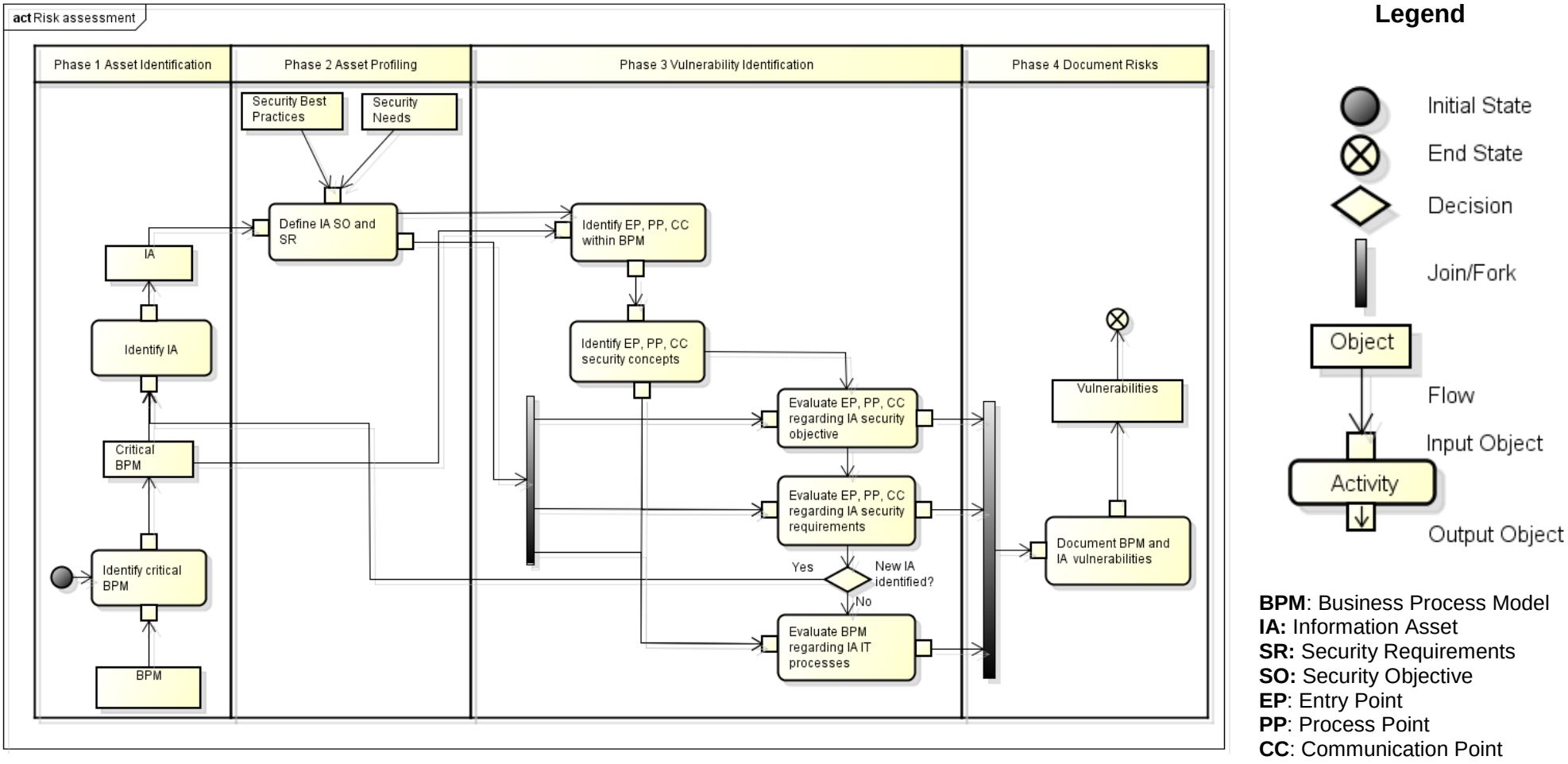


Figure A-32 Security requirements based risk assessment process (SRA) in UML

A.3. ARA Security checklist – Example

Table A-5: Control objectives at the ARA

1.	General IS awareness
1.1	User education and training Subject: Training organisation, program and performance
	Example questions: Check if employees are regular informed and trained about security topics. Check if security training (mandatory, used medium,...) are conducted.
1.2	User awareness Subject: Users awareness regarding information security
	Example questions: Are methods employed to make employees aware of security, i.e., posters, booklets, emails...? Interview employees about their awareness of security issues.
2.	IT management and IS compliance
2.1	IT processes, organisation and relationships Subject: Organisation chart, services and their descriptions
	Example questions: Check the Organisation chart that functions are segregated and business needs can be fulfilled. Check description/Implementation of IT Services.
2.2	Regulatory Compliance Subject: National or international tax, data or encryption regulations
	Example questions: Check if a local data protection law is known, in place and adhered to. Check if life data exists and is treated properly.
2.3	Data - Data ownership, Classification and Handling Subject: Regulations and measures for classification, storage and deletion of data
	Example questions: Check if a data lifecycle policy (retention periods) is existent and adhered to. Check if a data classification policy is available and adhered to.
3.	Systems security and operation management
3.1	Service Desk, incidents and problems Subject: Help desk activities, performance and service, Problem management
	Example questions: Check the process description for help desk activities. Check if service levels are agreed. Check if problem solutions are documented, proper stored and accessible
3.2	Configuration management - Hard-/Software Subject: Software releases, inventory, configuration and license management
	Example questions: Check the appropriateness of the configuration management solution. Check if the software documentation for each application is available, current and sufficient.
3.3	IT investment, performance and capacity Subject: IT cost monitoring and budget planning processes
	Example questions: Check if a budget and controlling process is in place, documented and approvals are

	done/available from management. Check if a regular reporting (costs) from accounting to IT and from IT to management exits.
3.4	Systems security - Infrastructure Audit subject: Infrastructure configuration and administration
	Example questions: Check if systems server, databases, router have been hardened and how system and patch status are monitored. Check any infrastructure maintenance contracts and their execution.
3.5	Systems security - desktop Subject: Desk Policy, configuration and administration
	Example questions: Check if a clean desk policy exists and is adhered to. Check the user access rights on desktops and if they can or have installed software.
3.6	Solutions and changes - software configuration Subject: Program configuration, controls and documentation
	Example questions: Check if appropriate system documentation is available for every application (short description, a general overview, a user manual, technical specifications, functional specifications, data flow diagrams, data structure diagram, test results and a approval and change documentation).
4.	Physical and logical access
4.1	User and Access Rights Management Subject: User access rights and processes
	Example questions: Check the process and documentation to gain and to withdraw access to applications and system. Check if access permissions to systems are in line with defined job/business requirements. Check segregation of duties in important applications and infrastructure systems.
4.2	Site design and access Subject: Physical access and maintenance of security measures
	Example questions: Check how access to the buildings is controlled and if access is logged. Check if a uninterruptible power supply and a air cooling system is installed, operational and sufficient. Check if fire detection devices, emergency lights, safety doors and fire extinguishers are installed and regularly maintained.
5.	Backup, disaster recovery and BCM
5.1	Data - backup Subject: Data-backup and restore processes and documentation
	Example questions: Check backup procedures (approach, daily tasks), documentation (systems, data, tools, approach) and backup equipment. Check the backup frequency, backup media tracking, storage of backups and retention periods of data.
5.2	Continuous service - recovery and planning Subject: Disaster and Contingency procedures and documentation
	Example questions: Check if a disaster recovery plan exists and whether the restore of systems (critical ones) and types of outages are described Check if business departments where involved in the disaster recovery tests. Check the conducted tests and the documentation of the tests.
6.	Software development and projects
6.1	Project management

	Subject: project management, plan and controlling
	Example questions: Check the overall management and planning of all projects Check project steering (PM and steering committee) and communication (team and business).
6.2	Software development Subject: Specifications, change management, test, data migration and conversion and release
	Example questions: Check the available procedures/processes for change, approval, test, quality assurance and release of developed software. Check test (test cases, test approach) and development (customization, change and defect solutions) approach.

A.4. Company assessments with the SRA and ARA

IT security risk assessments are performed by two security experts at subsidiaries of a global insurance company. The ARA and the SRA were both applied to processes (claims, accounting and underwriting) and systems of three distinct insurance entities. At the first entity, the ARA and SRA were applied successively, twice, by one assessor. At the second and third, the ARA and SRA were performed by the same people - now acting as a team. The information assets' security requirements were reused at each entity because the security needs for the assets did not change. Due to confidentiality reasons, the original business process models could not be presented. Remodelled business process models were used to show the results for the three areas examined – underwriting, accounting and claims - at the three entities. The same models are presented as, at the examined companies, business and the business segment (insurance non-life) are the same. Furthermore, global process blueprints were used for organising the business processes at these companies which differ only marginally from one another. In the following, the results of the assessors/teams at each entity are presented.

i. SRA Company 1 results – Assessor one

In this section the SRA assessment result of the 1st assessor at company one are presented.

Claims process evaluation (Company 1)

Table A-6, Table A-7 and Table A-8 show the assessment results of the claims sub-processes:

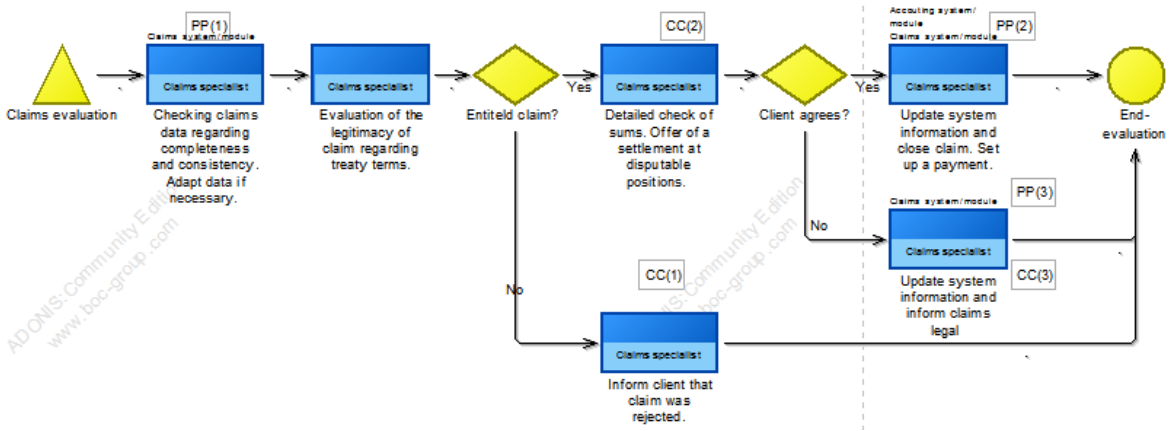


Figure A-33 Claims evaluation process

Table A-6: Claims evaluation results company 1 assessor 1

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): claims system	AC2	A4	D1	nok	ok	ok	nok	nok	ok	ok
PP(2): claims system	AC2	A4	D1	nok	ok	ok	nok	nok	ok	ok
PP(2): acc system	AC2	A3	D1	ok	ok	ok	ok	nok	ok	ok
PP(3): claims system	AC2	A4	D1	nok	ok	ok	nok	nok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): client / letter	C1	E2		ok	ok	n/a	ok	n/a	ok	ok
CC(2): client / letter	C1	E2		ok	ok	n/a	ok	n/a	ok	ok
CC(3): legal / email	C3	E1		ok	ok	ok	ok	ok	ok	ok

Result explanation: The PP1, PP2 and PP3 processing related to the claims system as well as the 'PiSys', at all PPs, was rated as nok because of the access authorisations and claims limits. The claims specialist has unrestricted access rights in the system; no claims limits are set up; and no authorisation activity is established in the system.

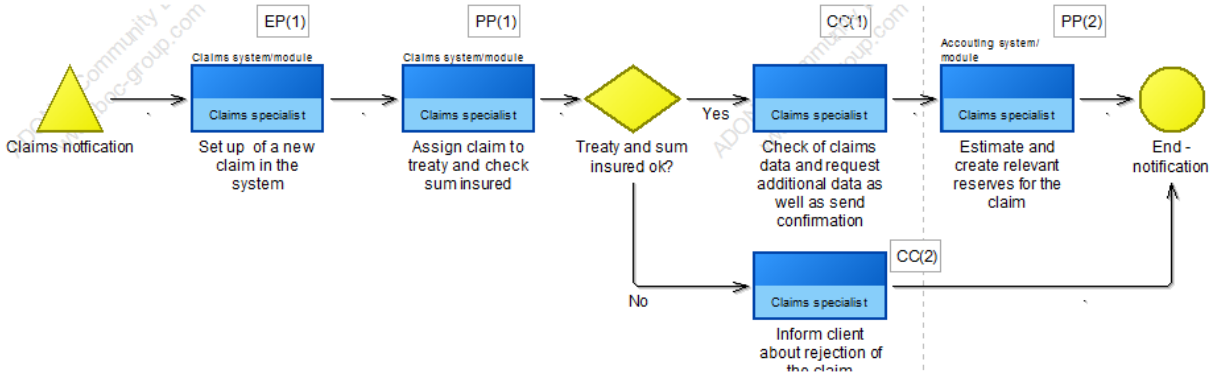


Figure A-34 Claims notification process

Table A-7: Claims notification results company 1 assessor 1

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): claims system	AC2	A4	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): claims system	AC2	A4	D2	ok	ok	ok	ok	ok	ok	ok
PP(2): acc system	AC2	A3	D2	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): cust. data	C1	E0		nok	nok	n/a	nok	n/a	nok	ok
CC(2): cust. data	C1	E0		nok	nok	n/a	nok	n/a	nok	ok

Result explanation: CC1 and CC2 processing and organisation were rated as nok because communication between the claims specialist and the client is insecure.

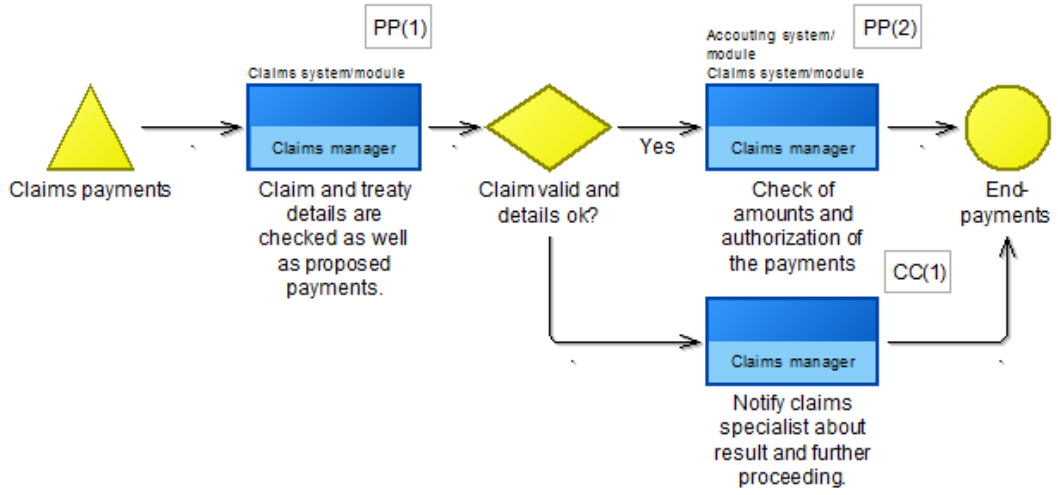


Figure A-35 Claims payments process

Table A-8: Claims payment results company 1 assessor 1

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): claims system	AC2	A2	D1	ok	ok	ok	ok	ok	ok	ok
PP(2): acc system	AC2	A3	D1	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): literally / email	C3	E0		ok	ok	n/a	ok	n/a	nok	nok

Result explanation: Organisation and physical were rated nok at CC1, because documents were not locked away. In particular, there was no policy regarding the confidentiality of paper documents in the claims area. Furthermore, the claims manager's security awareness on the confidentiality of data was not very distinct.

Accounting process evaluation (Company 1)

Table A-9, Table A-10, Table A-11 and Table A-12 show the assessment results of the accounting sub-processes:

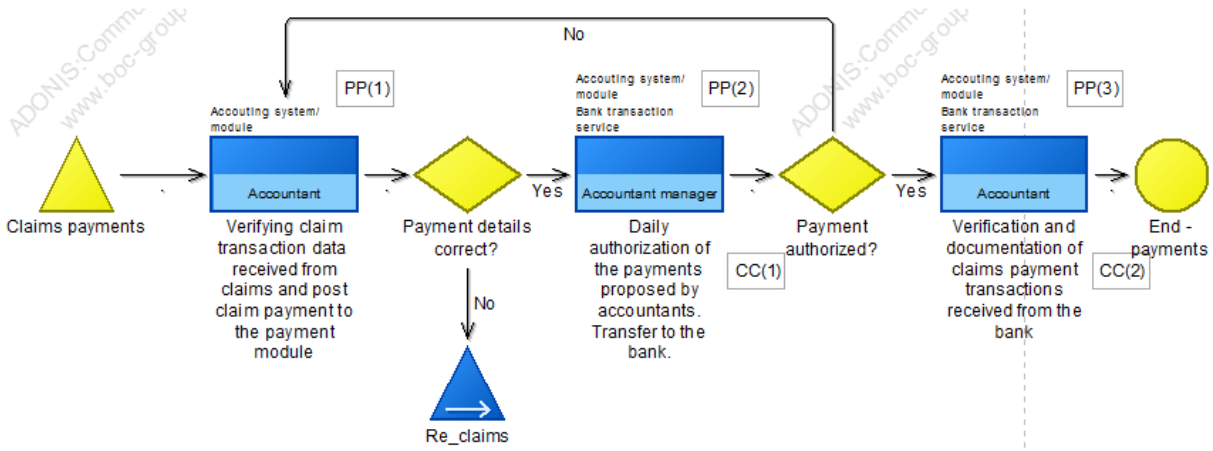


Figure A-36 Accounting claims payments process

Table A-9: Accounting payment results company 1 assessor 1

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): acc system	AC2	A3	D4	ok	ok	ok	ok	nok	nok	ok
PP(2): acc system	AC2	A2	D0	ok	ok	ok	ok	nok	ok	ok
PP(3): acc system	AC2	A3	D4	ok	ok	ok	ok	nok	nok	ok
CC	**A**	**E**					**CC**			
CC(1): bank service	C1	E1		nok	nok	ok	nok	ok	ok	n/a
CC(2): acc system	C1	E1		nok	nok	ok	nok	nok	ok	ok

Result explanation: The communication (CC1 and CC2) between the company and the bank was rated as nok because of the weak encryption. Because of wrongly implemented authorisations for the accounting manager, ‘PiSys’ was rated as nok at PP1 to PP3; likewise for organisation, expect at PP2. Accountants were able to authorise bookings in the system - not only the accounting manager.

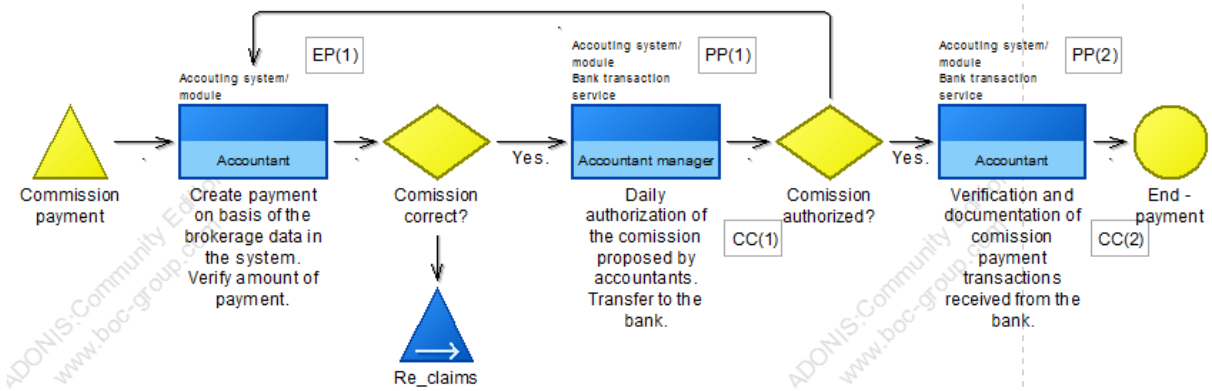


Figure A-37 Accounting commission payment process

Table A-10: Accounting commission payments results company 1 assessor 1

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): acc sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): acc sys	AC2	A2	D3	ok	ok	ok	ok	ok	ok	ok
PP(2): acc sys	AC2	A3	D4	ok	ok	ok	ok	nok	nok	ok
CC	**A**	**E**					**CC**			
CC(1): bank service	C1	E1		nok	nok	ok	nok	ok	ok	ok
CC(1): bank service	C1	E1		nok	nok	ok	nok	ok	ok	ok

Result explanation: The communication (CC1) between the company and the bank was rated as nok due to the weak encryption. Because of wrongly implemented authorisations, ‘PiSys’ and ‘Org’ were rated as nok at PP2. Accountants were able to authorise bookings in the system and not only the accounting manager.

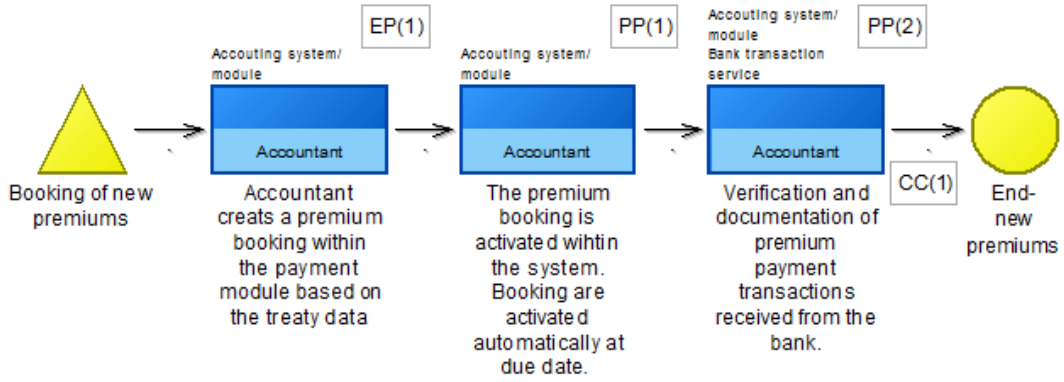


Figure A-38 Accounting booking of new premiums process

Table A-11: Accounting booking of new premiums results company 1 assessor 1

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): acc sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): acc sys	AC2	A2	D0	ok	ok	ok	ok	ok	ok	ok
PP(2): acc sys	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): bank service	C1	E1		nok	nok	ok	nok	ok	ok	ok

Result explanation: The communication (CC1) between the company and the bank was rated as nok because of the weak encryption.

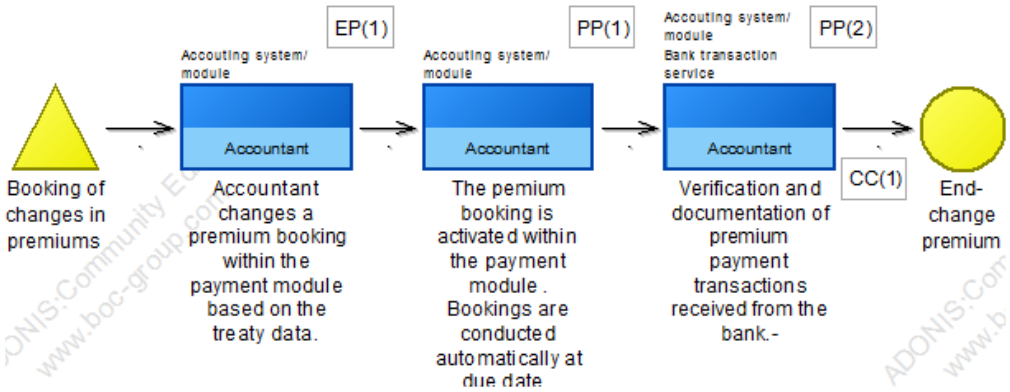


Figure A-39 Accounting booking of changes in premiums process

Table A-12: Accounting booking of changes in premiums results company 1 assessor 1

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): acc sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): acc sys	AC2	A2	D0	ok	ok	ok	ok	ok	ok	ok
PP(2): acc sys	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): bank service	C1	E1		nok	nok	ok	nok	ok	ok	ok

Result explanation: The communication (CC1) between the company and the bank was rated as nok because of the weak encryption.

Underwriting process evaluation (Company 1)

Table A-13, Table A-14 and Table A-15 show the assessment results of the underwriting sub-processes:

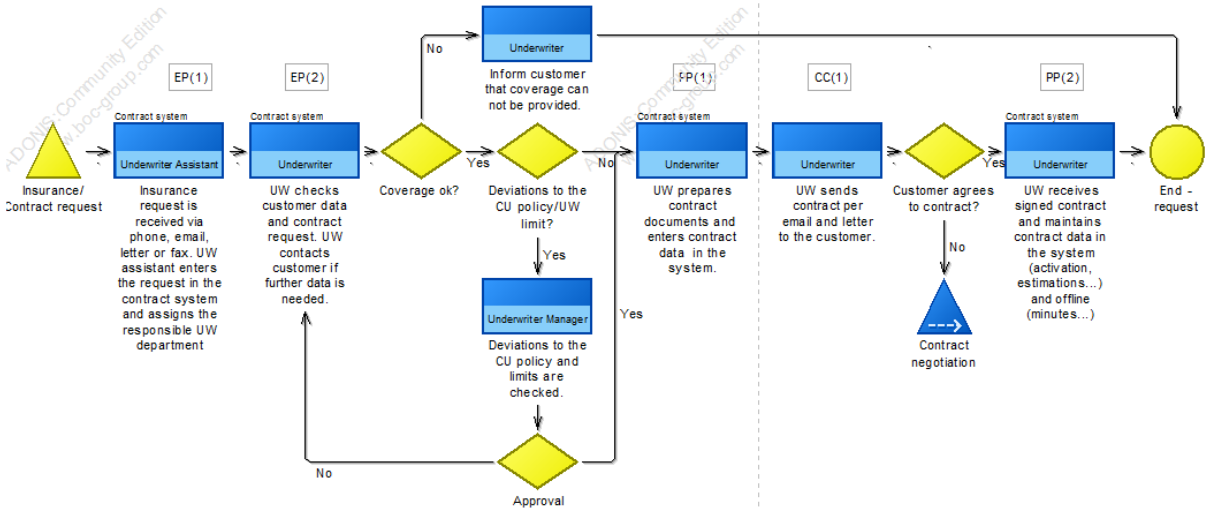


Figure A-40 Insurance/contract request process

Table A-13: Underwriting contract request and offer results company 1 assessor 1

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**

EP(1): contract sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
EP(2): contract sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): contract sys	AC2	A3	D3	ok	ok	ok	ok	ok	ok	ok
PP(2): contract sys	AC2	A3	D3	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): customer	C1	E0		nok	nok	ok	nok	ok	nok	ok

Result explanation: The communication (CC1) between the company and the customer was rated as nok, because they used email and post, and that the organisation (Org) was unaware of this.

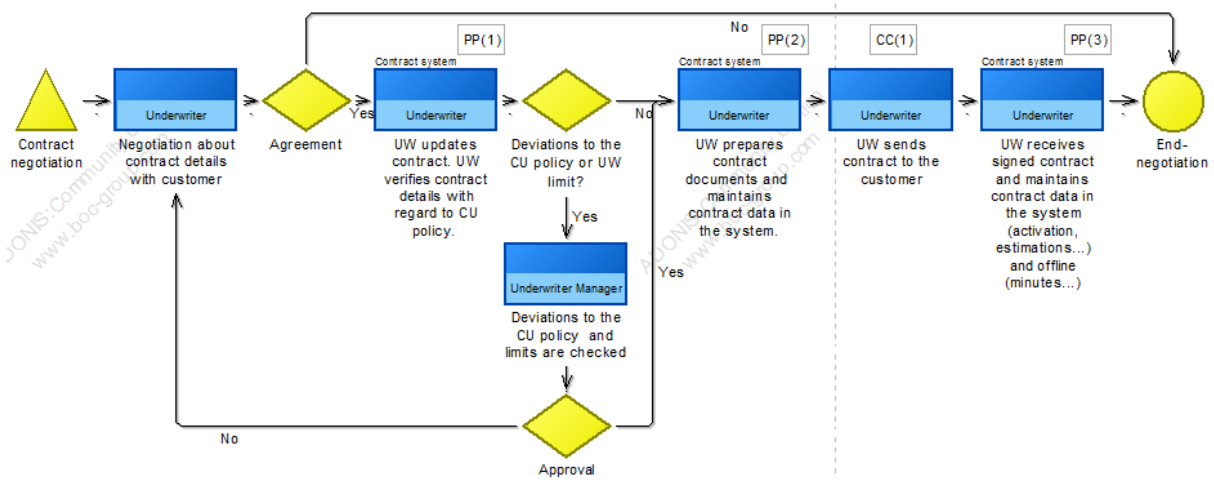


Figure A-41 Contract negotiation process

Table A-14: Underwriting contract negotiation results company 1 assessor 1

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): contract sys	AC2	A3	D3	ok	ok	ok	ok	nok	ok	ok
PP(2): contract sys	AC2	A3	D3	ok	ok	ok	ok	nok	nok	nok
PP(3): contract sys	AC2	A3	D3	ok	ok	ok	ok	nok	nok	nok
CC	**A**	**E**					**CC**			
CC(1): customer	C1	E0		nok	nok	ok	nok	ok	ok	ok

Result explanation: The communication (CC1) between the company and the customer was rated as nok at processing, because of the use of email and post. The contract system was rated as nok at 'PiSys' at PP1 to PP3, because the treaty verification is not implemented as specified. The organisation (Org) was rated as nok at these PPs where underwriters work on contracts; they are not aware of the confidentiality of data. This was identified in interviews. Furthermore, health data was found not securely locked away in our walkthrough, resulting in nok for 'Phy' at PP2 and PP3.

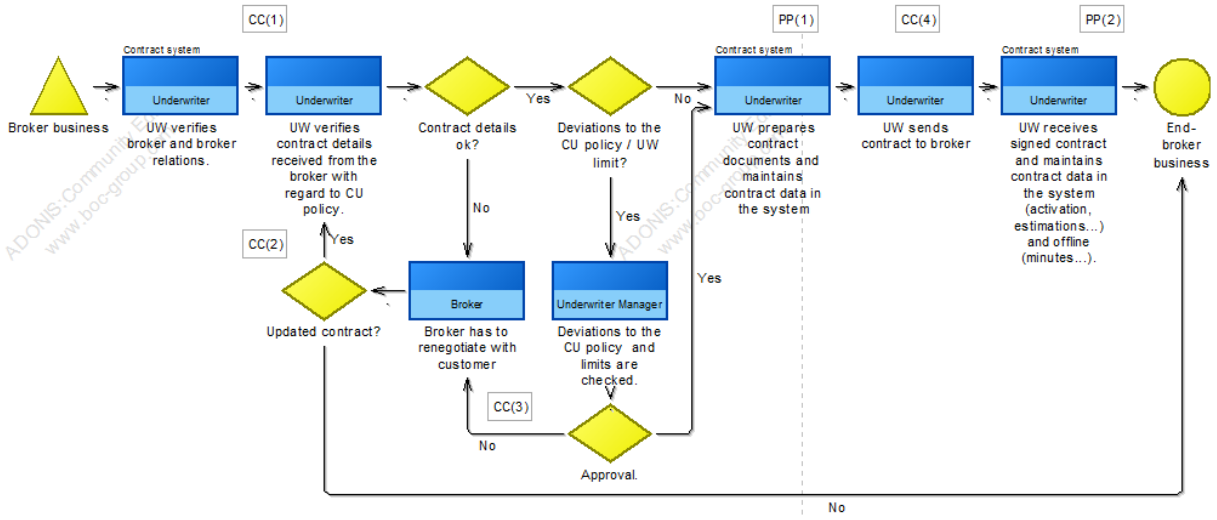


Figure A-42 Broker business process

Table A-15: Underwriting broker business results company 1 assessor 1

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): contract sys	AC2	A3	D3	ok	ok	ok	ok	nok	ok	ok
PP(2): contract sys	AC2	A3	D3	ok	ok	ok	ok	nok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): broker	C1	E1		nok	nok	ok	nok	n/a	ok	ok
CC(2): broker	C1	E1		nok	nok	ok	nok	n/a	ok	ok
CC(3): broker	C1	E1		nok	nok	ok	nok	n/a	ok	ok
CC(4): broker	C1	E1		nok	nok	ok	nok	n/a	ok	ok

Result explanation: The communication (C1 to CC4) between the underwriter and the broker was rated as nok at processing, because of the use of email and post. ‘PiSys’ at PP1 and PP2 was rated as nok because the treaty verification is not implemented as specified at the contract system.

Security process evaluation (Company 1 – assessor one)

The patch issue and the missing business continuity documentation were identified by checking the patch management and disaster recovery/business continuity processes. An analysis of the patch level revealed that the operating system of the accounting system misses several patches. In addition, some of the documentation referenced in the business continuity plan was not available and not up-to-date.

Table A-16: Security process assessment company 1

IT process name	Sub-process name or Control Objective	Evaluated	Affected Data	Identified issue
Service Strategy	Service Portfolio Management	no		
	Financial Management	no		
Service Design	Service Catalogue Management	no		
	Service Level Management	no		
	Risk Management	no		
	Capacity Management	yes	all	None
	Availability Management	yes	all	None
	IT Service Continuity Management	yes	all	Documentation was not up to date and not all applications were tested
	IT Security Management	yes	all	Patch issues were identified in this process as there were no current reports of the patch status. A conducted patch report revealed the patch issue
	Compliance Management	no		
	IT Architecture Management	no		

	Supplier Management	no		
Service Transition	Change Management	yes	all	None
	Project Management	no		
	Release and Deployment Management	no		
	Service Validation and Test	no		
	Application Development and Test	no		
	Service Asset and Configuration Management	no		
	Knowledge Management	no		
Service Operation	Event Management	no		
	Incident Management	no		
	Request Fulfilment	no		
	Access Management	yes	all	None
	Problem Management	no		
	IT Operations Management	yes	all	None
	IT Facilities Management	yes	all	None
Continual Service Improvement	Service Evaluation	no		
	Process Evaluation	no		
	Definition of Process Improvements	no		
	Tracking of Improvements	no		

Table A-17: Result presentation company 1 assessor 1

Processes/Issues – Information asset	Claims data	Accounting data	Underwriting data	Significance
Claims processes				
The claims specialist has unrestricted access to the claims system.	X			High
There are no claims limits set up in the system.	X			High
There is no authorisation activity in the process.				High
Paper documents were not securely stored in the Claims department.	X			Medium
Internal oral communication in the claims process was identified as not secure.	X			Low
Accounting processes				
Accountants can authorise bookings in the system but should not be able.		X		High
Data transfer between the bank and the company is insecure as only a weak encryption is used.		X		Medium
Underwriting processes				
There is no treaty data verification in the treaty system.			X	Low

Staff are not aware about IS threats.			X	Low
IT Security processes				
There is no appropriate disaster recovery and business continuity documentation.	X	X	X	Medium
The operating system of the accounting system misses several patches.		X		Medium

ii. SRA Company 1 results – Assessor two

In this section, the SRA assessment result of the second assessor at company one are presented.

Claims process evaluation (Company 1)

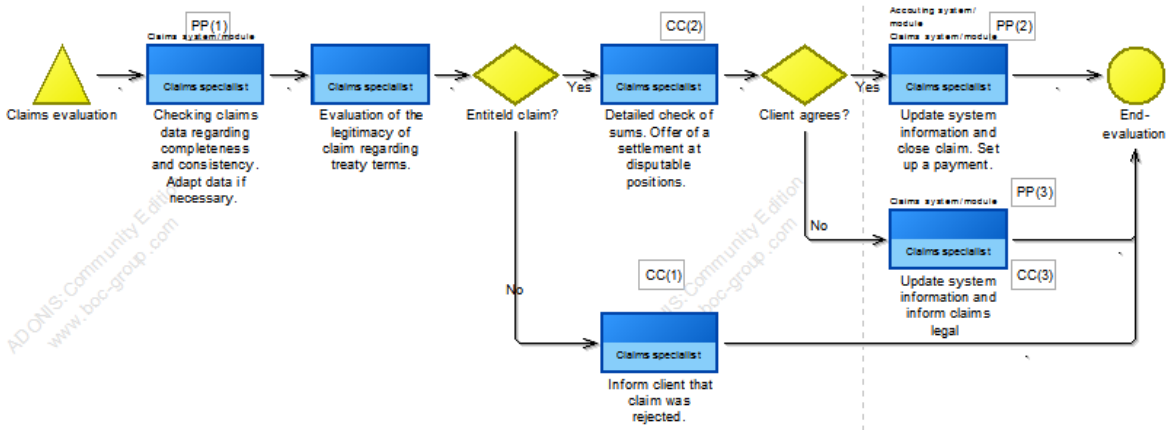


Figure A-43 Claims evaluation process

Table A-18: Claims evaluation results company 1 assessor 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): claims system	AC2	A4	D1	nok	ok	ok	nok	nok	ok	ok
PP(2): acc/claims system	AC2	A4	D1	nok	ok	ok	nok	nok	ok	ok
PP(3): claims system	AC2	A4	D1	nok	ok	ok	nok	nok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): client / letter	C1	E2		ok	ok	n/a	ok	n/a	ok	ok
CC(2): client / letter	C1	E2		ok	ok	n/a	ok	n/a	ok	ok
CC(3): legal / email	C3	E1		ok	ok	ok	ok	ok	ok	ok

Result explanation: The claims specialist has unrestricted access (full control) to the claims system without any further validation step of the changes made (thus, PP1 to PP3 processing result is nok). There are no claims limits set up, which means the claims specialist can create claims and payments of any amount ('PiSys' at PP1, PP2 and PP3 rated as nok).

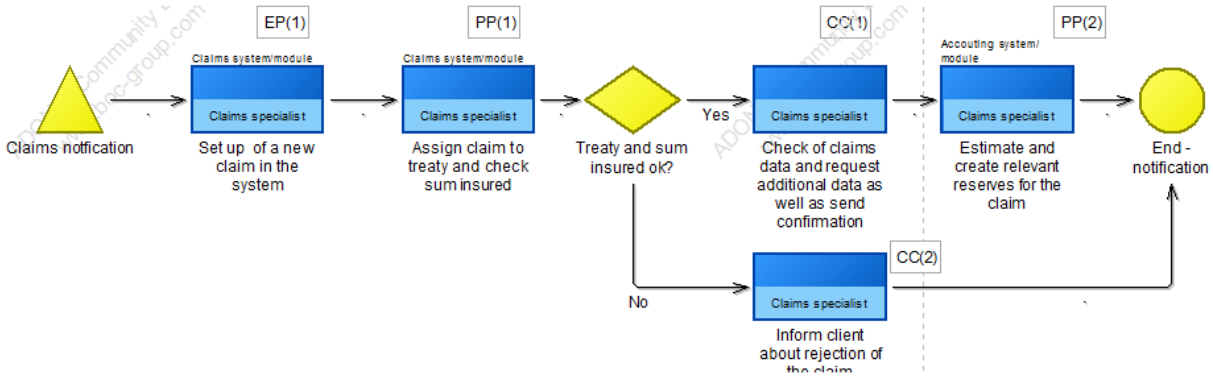


Figure A-44 Claims notification process

Table A-19: Claims notification results company 1 assessor 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): claims system	AC2	A4	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): claims system	AC2	A4	D2	ok	ok	ok	ok	ok	ok	ok
PP(2): acc system	AC2	A3	D2	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): cust. data	C1	E1		nok	nok	n/a	ok	n/a	ok	nok
CC(2): cust. data	C1	E1		nok	nok	n/a	ok	n/a	ok	ok

Result explanation: Claims data received is not stored securely, as observed in the claims area at CC1 'Phy'. The communication between the claims specialist and the customer via phone and post was rated as secure. Therefore, the CC1 and CC2 processing result was rated as ok, in contrast to the result for the security objectives.

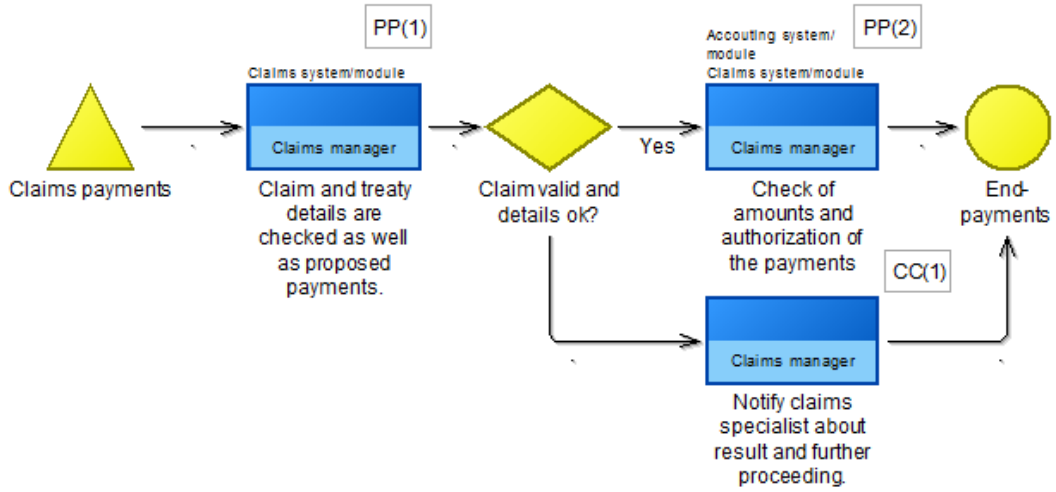


Figure A-45 Claims payments process

Table A-20: Claims payment results company 1 assessor 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): claims system	AC2	A2	D1	ok	ok	ok	ok	ok	ok	ok
PP(2): acc system	AC2	A3	D1	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): literally / email	C3	E2		ok	ok	n/a	ok	n/a	ok	ok

Result explanation: No issues identified.

Accounting process evaluation (Company 1)

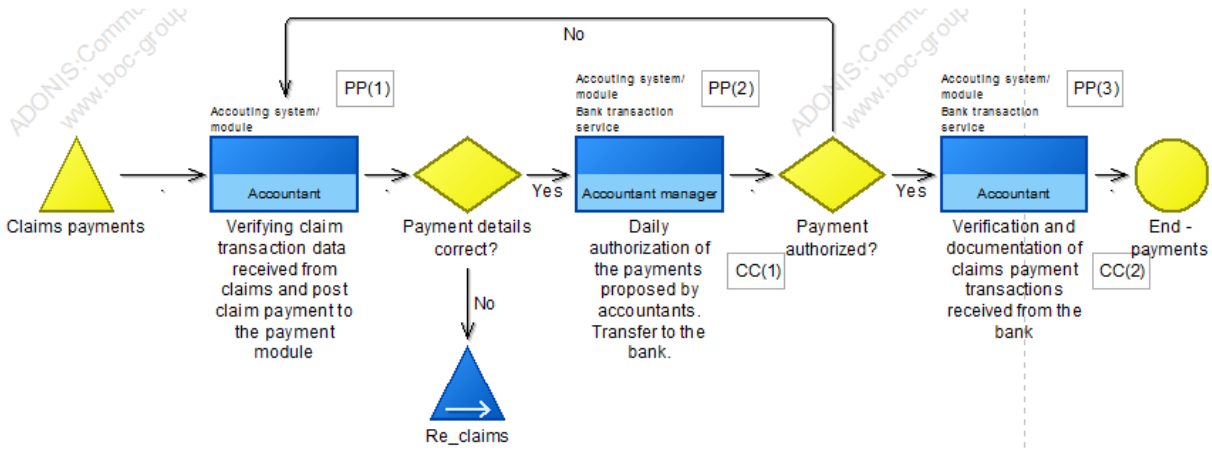


Figure A-46 Accounting claims payments process

Table A-21: Accounting payment results company 1 assessor 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1):acc system	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
PP(2):acc system	AC2	A2	D0	ok	ok	ok	ok	ok	ok	ok
PP(3):acc system	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): bank service	C1	E1		nok	nok	ok	nok	ok	ok	n/a
CC(2): acc system	C1	E1		nok	nok	ok	nok	ok	ok	ok

Result explanation: Weak encryption is used between the accounting system and the bank service. The requirements are not met by the encryption algorithm used rated as E1, leading to weak encryption at CC1 and CC2.

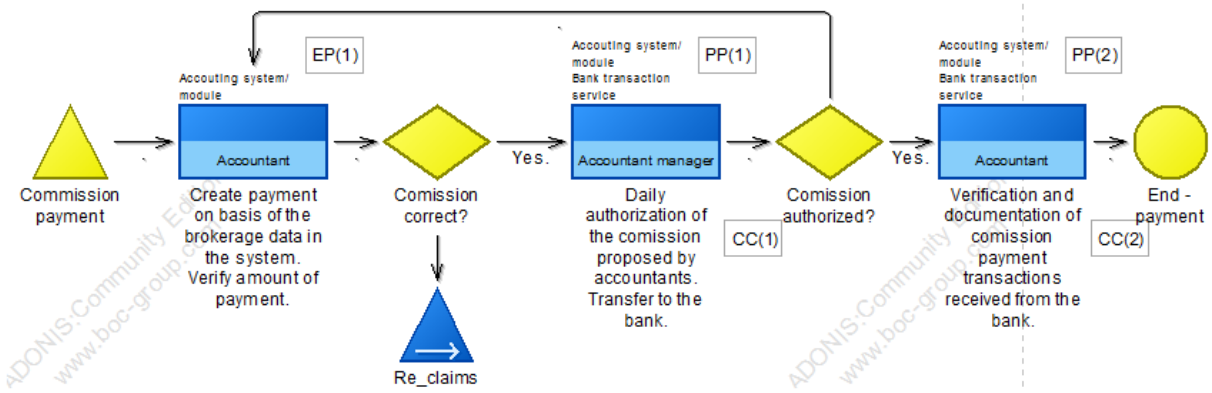


Figure A-47 Accounting commission payment process

Table A-22: Accounting commission payments results company 1 assessor 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**		**PiSys**	**Org**	**Phy**
EP(1): acc sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP										
PP(1): acc sys	AC2	A2	D3	ok	ok	ok	ok	ok	ok	ok
PP(2): acc sys	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**								
CC(1): bank service	C1	E1		nok	nok	ok	nok	ok	ok	ok
CC(2): bank service	C1	E1		nok	nok	ok	nok	ok	ok	ok

Result explanation: Weak encryption is used between the accounting system and the bank service. The requirements are not met by the encryption algorithm used (rated as E1 at CC1 and CC2), resulting in nok at the processing stage.

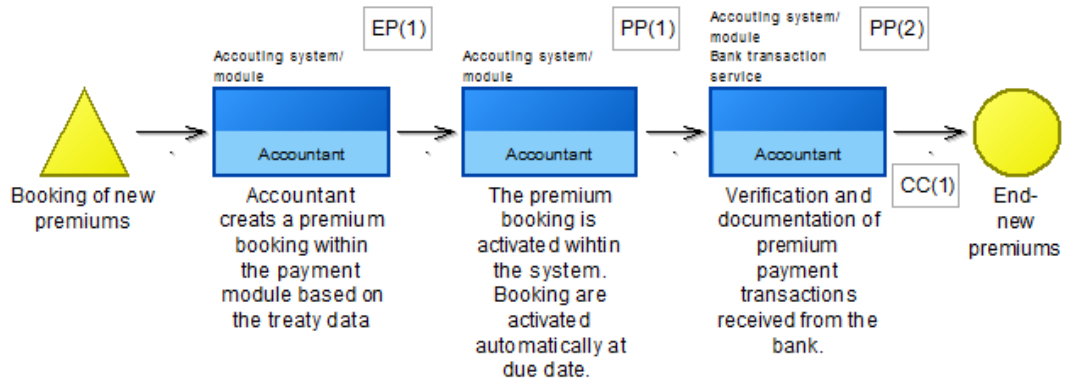


Figure A-48 Accounting booking of new premiums process

Table A-23: Accounting booking of new premiums results company 1 assessor 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): acc sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): acc sys	AC2	A2	D0	ok	ok	ok	ok	ok	ok	ok
PP(2): acc sys	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): bank service	C1	E1		nok	nok	ok	nok	ok	ok	ok

Result explanation: Weak encryption is used between the accounting system and the bank service. The requirements are not met by the encryption algorithm used rated as E1 at CC1; this results in nok at processing.

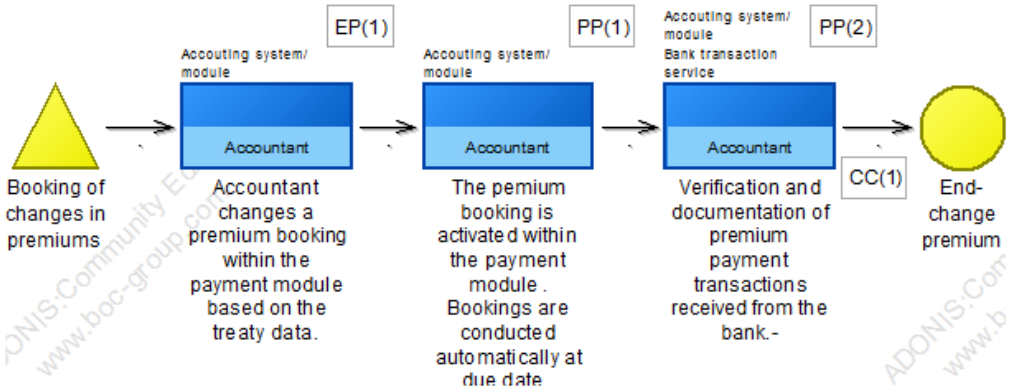


Figure A-49 Accounting booking of changes in premiums process

Table A-24: Accounting booking of changes in premiums results company 1 assessor 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**		**PiSys**	**Org**	**Phy**
EP(1): acc sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP										
PP(1): acc sys	AC2	A2	D0	ok	ok	ok	ok	ok	ok	ok
PP(2): acc sys	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**								
CC(1): bank service	C1	E1		nok	nok	ok	nok	ok	ok	ok

Result explanation: Weak encryption is used between the accounting system and the bank service. The requirements are not met by the encryption algorithm rated as E1 at CC1.

Underwriting process evaluation (Company 1)

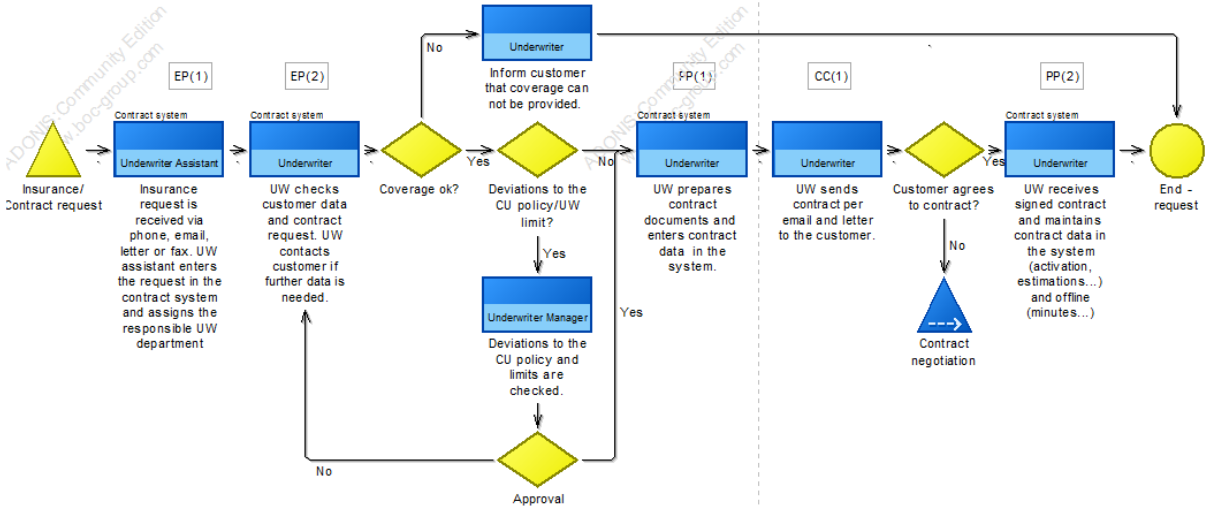


Figure A-50 Insurance/contract request process

Table A-25: Underwriting contract request and offer results company 1 assessor 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): contract sys	AC2	A3	D1	ok		ok	ok	nok	ok	nok
EP(2): contract sys	AC2	A3	D0	nok		ok	nok	nok	ok	ok
PP							**PP**			
PP(1): contract sys	AC2	A3	D3	ok	ok	ok	ok	nok	ok	ok
PP(2): contract sys	AC2	A3	D3	ok	ok	ok	ok	nok	ok	nok
CC	**A**	**E**					**CC**			
CC(1): customer	C1	E1		nok	nok	ok	ok	ok	ok	ok

Result explanation: Even if the security objectives of CC1 are rated as nok, the overall rating for CC1 is ok as other encryption possibilities are not deemed as feasible. Underwriters and Assistants do not have documents locked away (Phy nok at EP1 and PP2). Underwriters have not always verified the details in the

system with the contract request (nok at EP2 processing). Furthermore, the contract system does not provide any data verification functionality to identify any missing contract data during entry or processing of the data (PiSys rated nok at EPs and PPs).

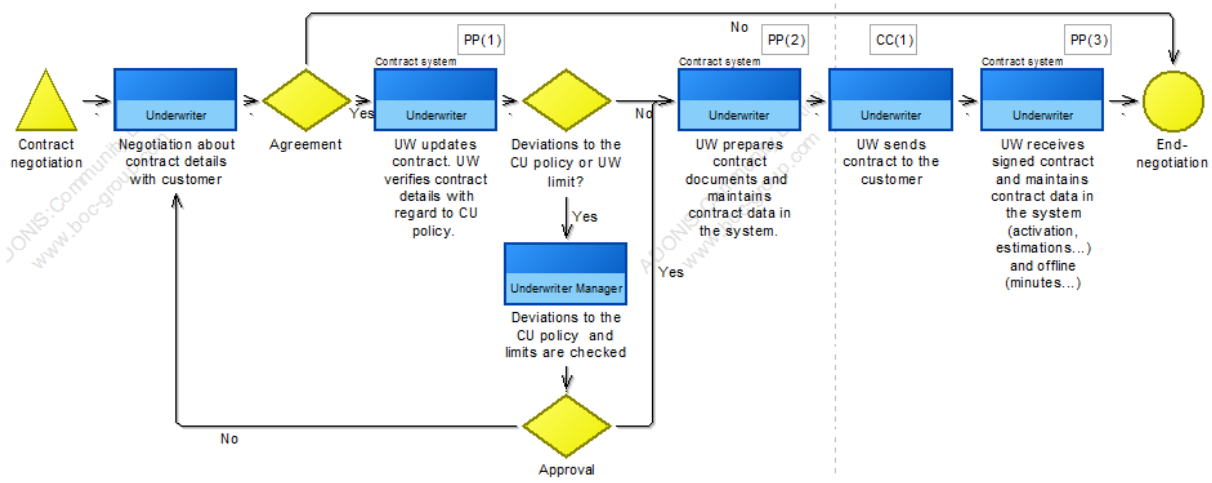


Figure A-51 Contract negotiation process

Table A-26: Underwriting contract negotiation results company 1 assessors 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): contract sys	AC2	A3	D1	ok	ok	ok	ok	nok	ok	ok
PP(2): contract sys	AC2	A3	D1	ok	ok	ok	ok	nok	ok	ok
PP(3): contract sys	AC2	A3	D1	ok	ok	ok	ok	nok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): customer	C1	E0		nok	nok	ok	ok	ok	ok	ok

Result explanation: Even if the security objectives of CC1 are rated as nok, the overall rating for CC1 is ok as other encryption possibilities are not deemed as feasible. The contract system does not provide any data verification functionality (PiSys rated nok at PP1 to PP3).

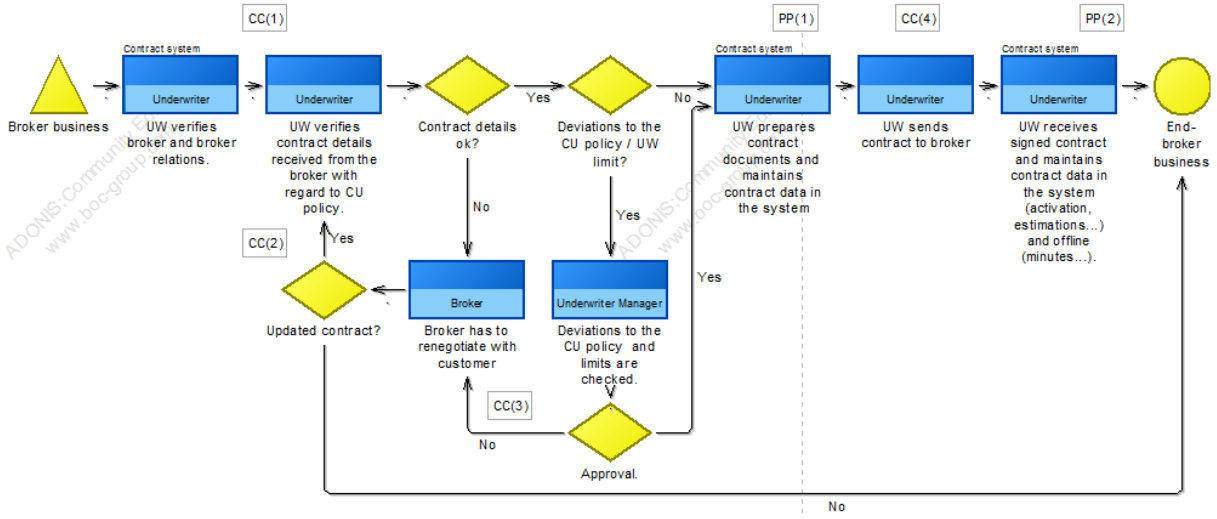


Figure A-52 Broker business process

Table A-27: Underwriting broker business results company 1 assessor 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): contract sys	AC2	A3	D3	ok	ok	ok	ok	nok	ok	ok
PP(2): contract sys	AC2	A3	D3	ok	ok	ok	ok	nok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): broker	C1	E1		nok	nok	ok	ok	n/a	ok	ok
CC(2): broker	C1	E1		nok	nok	ok	ok	n/a	ok	ok
CC(3): broker	C1	E1		nok	nok	ok	ok	n/a	ok	ok
CC(4): broker	C1	E1		nok	nok	ok	ok	n/a	ok	ok

Result explanation: Even if the security objectives are rated as nok at CC1 to CC4, the overall rating for all CCs is ok, as other encryption possibilities are not deemed as feasible. The contract system does not provide any data verification functionality (PiSys rated nok at PP1 and PP2).

Security process evaluation (Company 1)

Table A-28: Security process evaluation results

IT process name	Sub-process name or Control Objective	Evaluated	Affected Data	Identified issue
Service Strategy	Service Portfolio Management	no		
	Financial Management	no		
Service Design	Service Catalogue Management	no		
	Service Level Management	no		
	Risk Management	no		
	Capacity Management	No		
	Availability Management	No		
	IT Service Continuity Management	yes	all	The BCM documentation did miss some important details, e.g. the restore of systems was not described
	IT Security Management	yes	all	The patch report showed that not all servers had the most current patches applied. Some of the patches were rated high
	Compliance Management	no		
	IT Architecture Management	no		
	Supplier Management	no		
Service Transition	Change Management	yes	all	None
	Project Management	no		
	Release and Deployment Management	no		
	Service Validation and Test	no		
	Application Development and Test	no		
	Service Asset and Configuration Management	no		
	Knowledge Management	no		
Service Operation	Event Management	no		
	Incident Management	no		
	Request Fulfilment	no		
	Access Management	yes	all	None
	Problem Management	no		
	IT Operations Management	yes	all	None
	IT Facilities Management	yes	all	None
Continual Service Improvement	Service Evaluation	no		
	Process Evaluation	no		
	Definition of Process Improvements	no		
	Tracking of Improvements	no		

Table A-29: Results of company 1 assessor 2

Processes/Issues – Information asset	Claims data	Accounting data	Underwriting data	Significance
Claims processes				
Unrestricted access in the claims system. (Claims evaluation process)	X			High
Claims limits are not reflected in the system or process. (Claims evaluation process)	X			High
No secure storage of documents. (Claims notification process)	X			Low
Accounting processes				
Weak encryption is used. (All accounting processes)		X		Medium
Underwriting processes				
Treaty data is not verified in the system. (All underwriting processes)			X	Low
Information is insecurely treated by staff. (Contract request process)			X	Low
IT Security processes				
Disaster recovery and business continuity documentation insufficient.	X	X	X	Low
Several patches missing on systems.		X		Medium

iii. SRA Company 2 results

Claims process evaluation (Company 2)

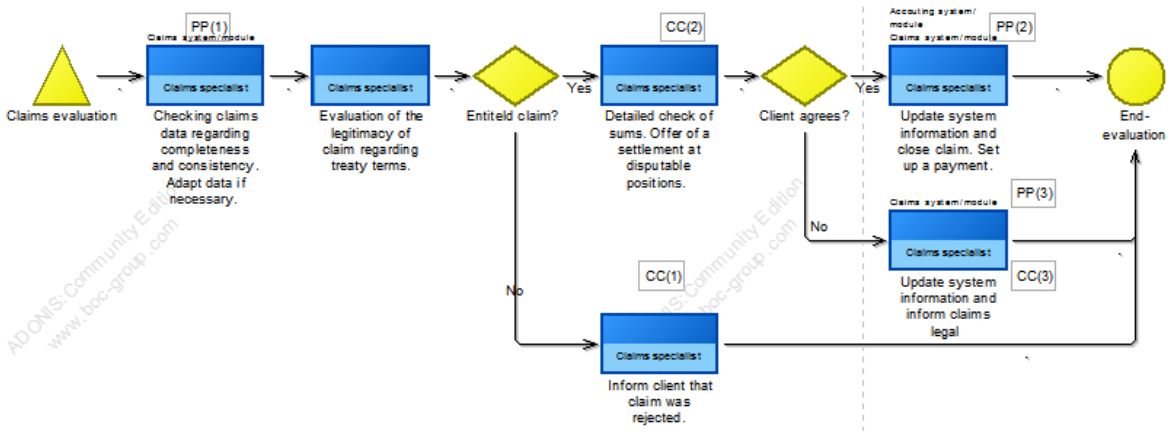


Figure A-53 Claims evaluation process

Table A-30: Claims evaluation results company 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): claims system	AC2	A4	D2	ok	ok	ok	ok	nok	ok	ok
PP(2): claims system	AC1	A4	D2	nok	nok	ok	ok	nok	ok	ok
PP(2): acc system	AC2	A3	D2	ok	ok	ok	ok	nok	ok	ok
PP(3): claims system	AC2	A4	D2	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): client / letter	C1	E2		ok	ok	n/a	ok	n/a	ok	ok
CC(2): client / letter	C1	E2		ok	ok	n/a	ok	n/a	ok	ok
CC(3): legal / email	C3	E1		ok	ok	ok	ok	ok	ok	ok

Result explanation: For the calculation of claims and the loss history, spreadsheets are used without any access and change controls. Therefore, PiSys (claims and accounting system) was rated as nok at PP1 and PP2.

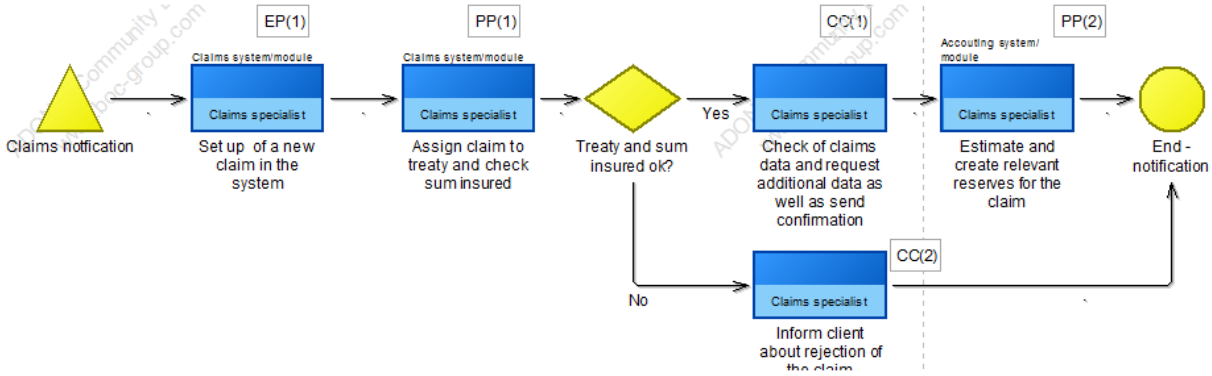


Figure A-54 Claims notification process

Table A-31: Claims notification results company 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): claims system	AC2	A4	D0	nok		ok	nok	nok	nok	ok
PP							**PP**			

PP(1): claims system	AC2	A4	D2	ok	ok	ok	ok	ok	ok	ok
PP(2): acc system	AC2	A3	D2	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): cust. data	C1	E3		ok	ok	n/a	ok	n/a	nok	ok
CC(2): cust. data	C1	E3		ok	ok	n/a	ok	n/a	nok	ok

Result explanation: Claims data entry is not checked for completeness and misses information with regard to the claim occurred (EP1 processing rated nok). Furthermore, PiSys and Org were rated as nok at EP1, as the claims data were not checked accordingly and further data not requested.

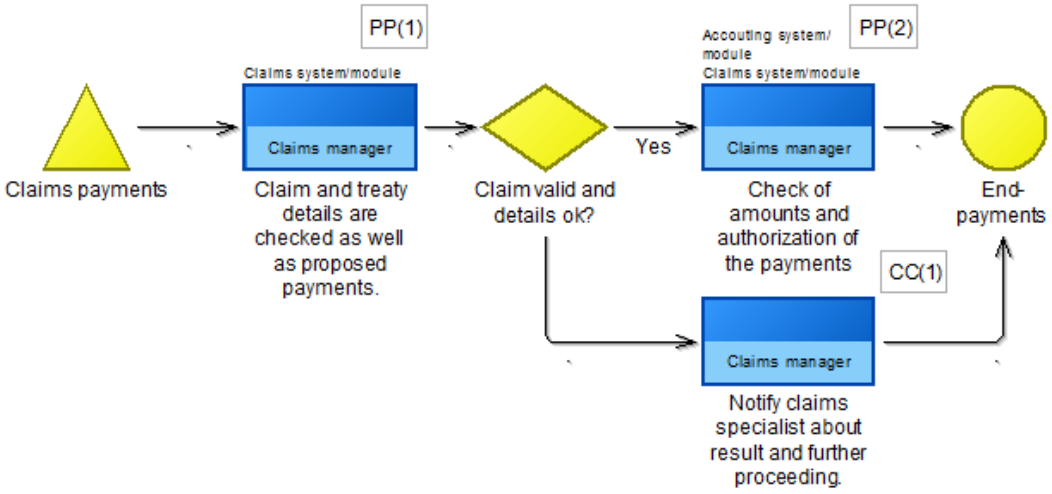


Figure A-55 Claims payments process

Table A-32: Claims payment results company 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): claims system	AC2	A2	D1	ok	ok	ok	ok	ok	ok	ok
PP(2): acc system	AC2	A3	D1	ok	ok	ok	ok	ok	nok	ok
CC	**A**	**E**					**CC**			
CC(1): literally / email	C3	E0		ok	ok	n/a	ok	n/a	ok	ok

Result explanation: The claims specialist is able to release claims payments in the accounting system without any authorisation in the system. Therefore, Org at PP2 was rated as nok.

Accounting process evaluation (Company 2)

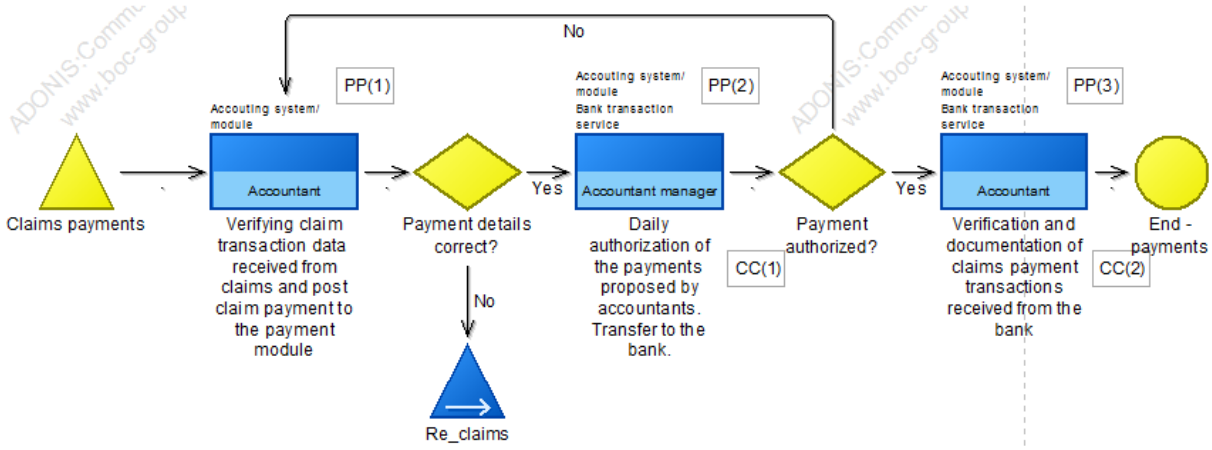


Figure A-56 Accounting claims payments process

Table A-33: Accounting payment results company 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): acc system	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
PP(2): acc system	AC2	A2	D1	ok	ok	ok	ok	ok	ok	ok
PP(3): acc system	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): bank service	C1	E2		ok	ok	ok	ok	ok	ok	n/a
CC(2): acc system	C1	E2		ok	ok	ok	ok	ok	ok	ok

Result explanation: No issues found.

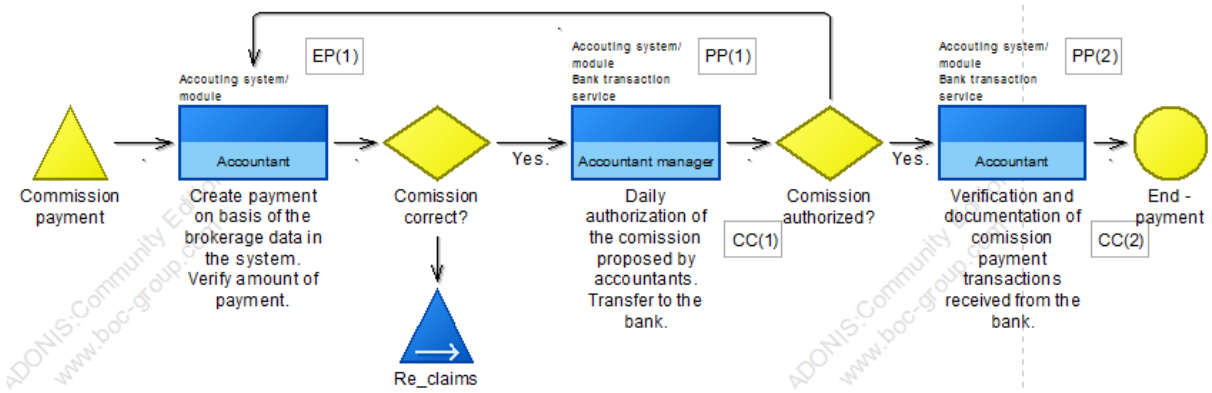


Figure A-57 Accounting commission payment process

Table A-34: Accounting commission payments results company 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): acc sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): acc sys	AC2	A2	D3	ok	ok	ok	ok	ok	ok	ok
PP(2): acc sys	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): bank service	C1	E2		ok	ok	ok	ok	ok	ok	ok
CC(1): bank service	C1	E2		ok	ok	ok	ok	ok	ok	ok

Result explanation: No issues found.

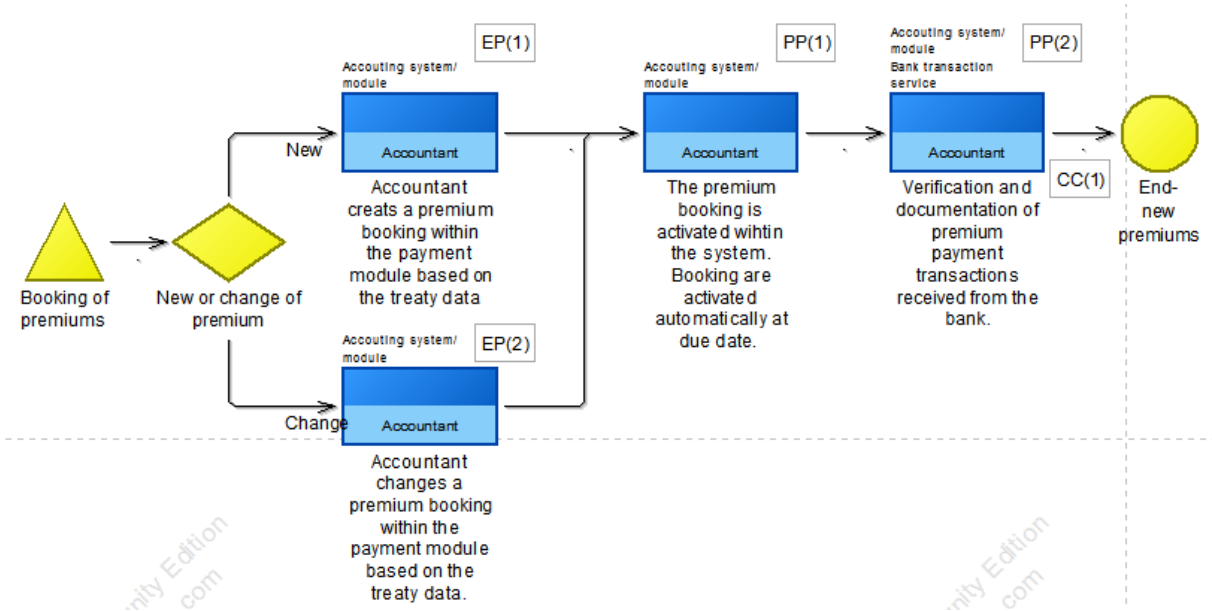


Figure A-58 Accounting booking of new and changes in premiums

Table A-35: Accounting booking of new and changes in premiums results company 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): acc sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
EP(2): acc sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1):acc sys	AC2	A2	D1	ok	ok	ok	ok	ok	ok	ok
PP(2):acc sys	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): bank service	C1	E2		ok	ok	ok	ok	ok	ok	ok

Result explanation: No issues found.

Underwriting process evaluation (Company 2)

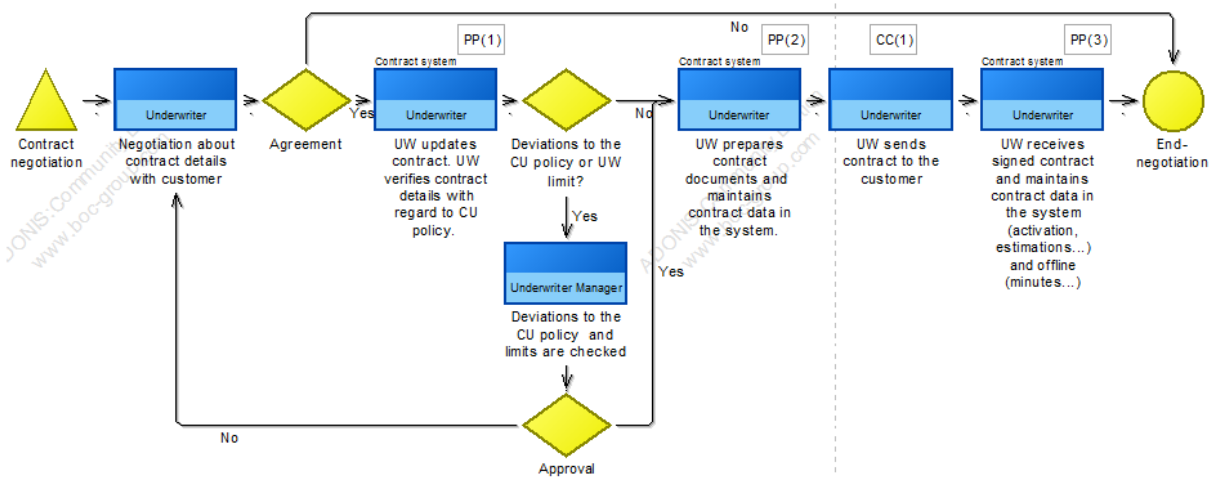


Figure A-59 Contract negotiation process

Table A-36: Underwriting contract negotiation results company 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): contract sys	AC2	A4	D1	nok	ok	ok	nok	nok	nok	ok
PP(2): contract sys	AC2	A4	D1	nok	ok	ok	nok	nok	ok	ok

PP(3): contract sys	AC2	A4	D1	nok	ok	ok	nok	nok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): customer	C1	E1		ok	ok	ok	ok	ok	ok	ok

Result explanation: There is no alignment between Underwriting and Actuarial services. There are cases where the Underwriter has to contact Actuarial services for guidance. Furthermore, deviations to the Corporate Underwriting policy, for example, have to be authorised. However, this is not appropriately modelled. The model and the systems used do not fully reflect this. Therefore, the PiSys at PP1 to PP3 and Org at PP1 were rated as nok. In addition, the integrity of contract information is endangered as there is full control access in the contract system without a proper data validation activity, resulting in a rating of nok at the integrity security objective and PP1 to PP3 processing result.

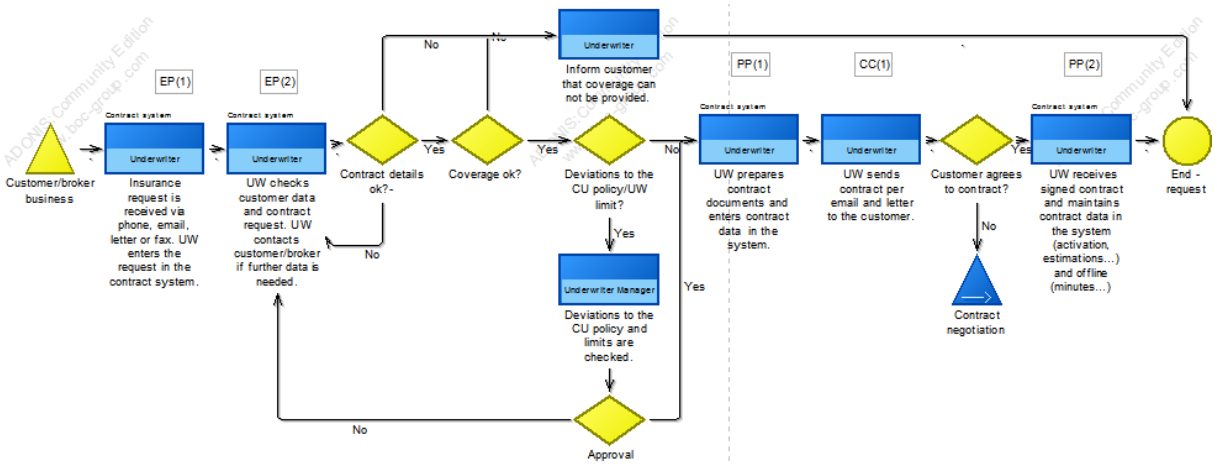


Figure A-60 Customer and broker business process

Table A-37: Underwriting customer and broker business results company 2

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): contract sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok

EP(1): contract sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): contract sys	AC2	A3	D3	ok	ok	ok	ok	nok	nok	ok
PP(2): contract sys	AC2	A3	D3	ok	ok	ok	ok	nok	nok	ok
CC	**A**	**E**					**CC**			
CC(1): customer	C1	E2		ok	ok	ok	ok	n/a	ok	ok

Result explanation: There is no authorisation activity for entering and release of customer and broker business. PiSys and Org were rated as nok at PP1 and PP2. There is no alignment between Underwriting and Actuarial services. There are cases where the Underwriter has to contact Actuarial services for guidance. However, this is not appropriately modelled.

Security process evaluation (Company 2)

Table A-38: Security process evaluation results

IT process name	Sub-process name or Control Objective	Evaluated	Affected Data	Identified issue
Service Strategy	Service Portfolio Management	no		
	Financial Management	no		
Service Design	Service Catalogue Management	no		
	Service Level Management	no		
	Risk Management	no		
	Capacity Management	yes	all	None
	Availability Management	yes	all	None
	IT Service Continuity Management	yes	all	The disaster recovery documentation misses testing scenarios
	IT Security Management	yes	all	Interviews revealed that people are not aware of their responsibilities
	Compliance Management	no		
	IT Architecture Management	no		
	Supplier Management	no		
Service Transition	Change Management	yes	all	None
	Project Management	no		
	Release and Deployment Management	no		
	Service Validation and Test	no		
	Application Development and Test	no		

	Service Asset and Configuration Management	no		
	Knowledge Management	no		
Service Operation	Event Management	no		
	Incident Management	no		
	Request Fulfilment	no		
	Access Management	yes	all	The access rights process for systems was not followed in several cases. Access to claims system was unrestricted because of a deficiency in the role model
	Problem Management	no		
	IT Operations Management	yes	all	BCM/DR plans were not tested. The daily procedures checklist used for server operation management was not followed and checked accordingly
	IT Facilities Management	yes	all	During the walkthrough unsecured information was found on desks/in the office
Continual Service Improvement	Service Evaluation	no		
	Process Evaluation	no		
	Definition of Process Improvements	no		
	Tracking of Improvements	no		

Table A-39: Result presentation company 2

Processes/Issues – Information asset	Claims data	Accounting data	Underwriting data	Significance
Claims processes				
The claims specialist is able to release claims without authorisations in the system. (Claims payment process)	X			High
Process of claims data entry is inappropriate due to missing claims information. (Claims notification process)	X			High
Used spreadsheets for claims calculation - no access and change controls. (Claims evaluation process)	X			Medium
Claims data received were not properly checked. (Claims notification process)	X			Medium
Underwriting processes				
Missing alignment between Underwriter and Actuarial services for contract pricing. (Customer and broker business process)			X	Medium

Broker approval process was to work as designed. (Customer and broker business process)	X		X	Medium
Missing authorisation for underwriting policy deviations. (Contract negotiation process)			X	High
IT security processes				
There is no updated disaster recovery plan.	X	X	X	Low
The BCM/DR activities were not tested appropriately.	X	X	X	Medium
The system access approval process for claims system was not adequate as unlimited access was granted immediately. (Contract negotiation process and security processes	X			Medium
The daily procedures in the system operation centre were not processed as required.				Medium
In interviews it was found that data owners are not aware of their responsibilities with regard to applications and the system access.				Low
Some paper documents which contained confidential information were not stored in locked cabinets.	X	X	X	Low

iv. SRA Company 3 results

Claims process evaluation (Company 3)

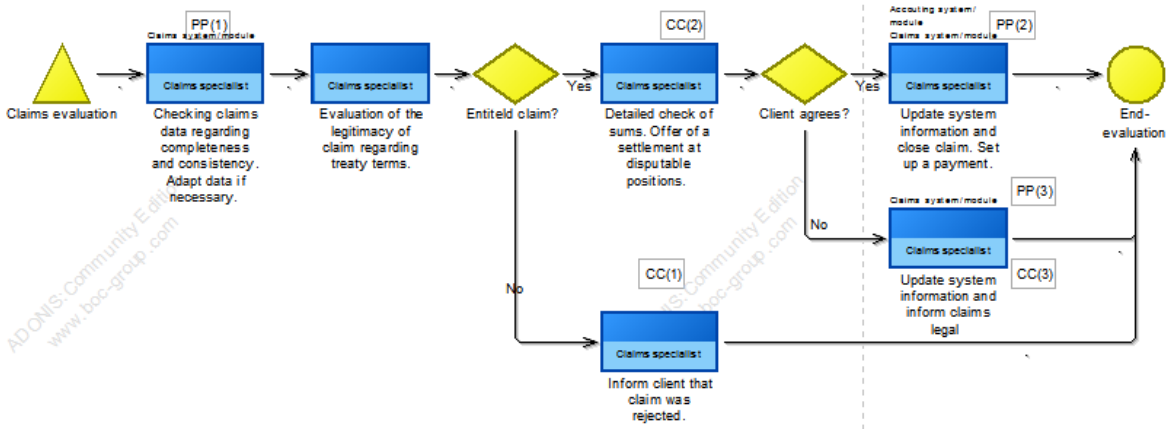


Figure A-61 Claims evaluation process

Table A-40: Claims evaluation results company 3

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): claims system	AC2	A4	D2	ok	ok	ok	ok	ok	ok	ok
PP(2): acc system	AC2	A3	D2	ok	ok	ok	ok	ok	ok	ok
PP(3): claims system	AC2	A4	D2	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): client / letter	C1	E2		ok	ok	n/a	ok	n/a	ok	ok
CC(2): client / letter	C1	E2		ok	ok	n/a	ok	n/a	ok	ok
CC(3): legal / email	C3	E1		ok	ok	ok	ok	ok	ok	ok

Result explanation: No issues found.

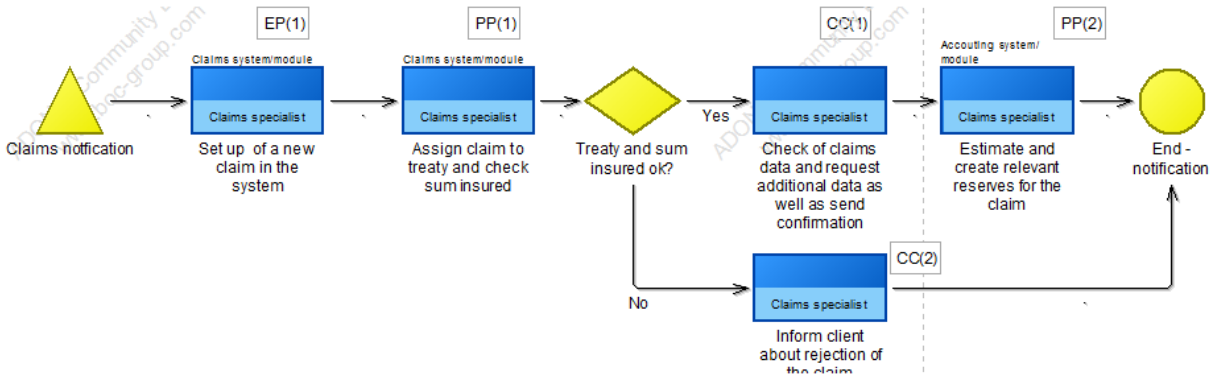


Figure A-62 Claims notification process

Table A-41: Claims notification results company 3

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): claims system	AC2	A4	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): claims system	AC2	A4	D2	ok	ok	ok	ok	ok	ok	ok
PP(2): acc system	AC2	A3	D2	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): cust. data	C1	E3		ok	ok	n/a	ok	n/a	ok	ok
CC(2): cust. data	C1	E3		ok	ok	n/a	ok	n/a	ok	ok

Result explanation: No issues found.

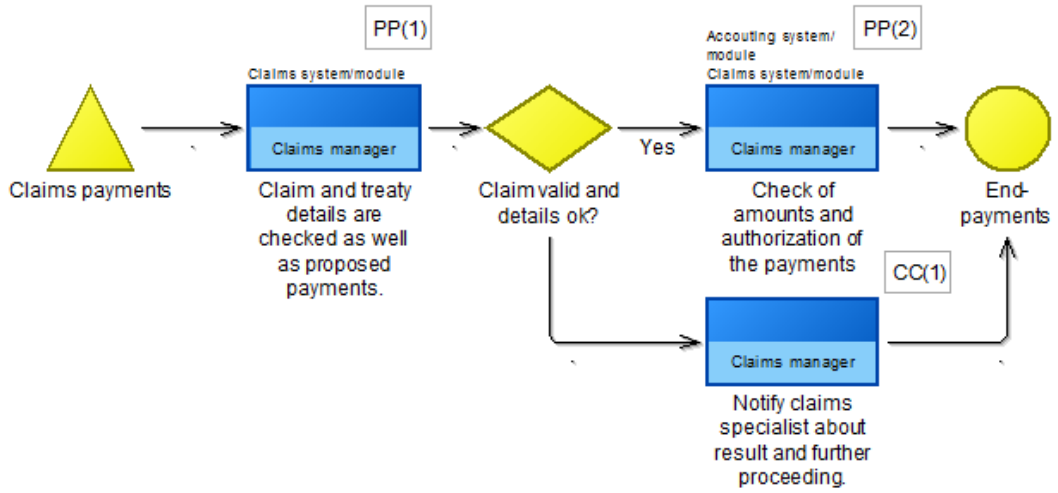


Figure A-63 Claims payments process

Table A-42: Claims payment results company 3

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): claims system	AC2	A2	D1	ok	ok	ok	ok	ok	ok	ok
PP(2): acc system	AC2	A3	D1	ok	ok	ok	ok	nok	nok	ok
CC	**A**	**E**					**CC**			
CC(1): literally / email	C3	E0		ok	ok	n/a	ok	n/a	ok	ok

Result explanation: Claims are not authorised accordingly by the claims manager. PiSys and Org are thus rated as nok at PP2.

Accounting process evaluation (Company 3)

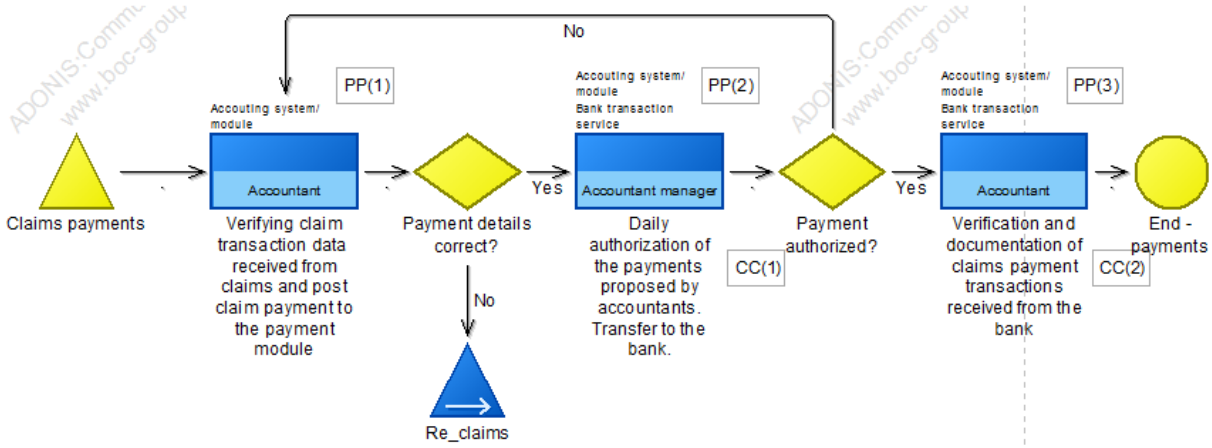


Figure A-64 Accounting claims payments process

Table A-43: Accounting payment results company 3

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): acc system	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok

PP(2): acc system	AC2	A2	D1	ok	ok	ok	ok	nok	ok	ok
PP(3): acc system	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): bank service	C1	E2		ok	ok	ok	ok	ok	ok	n/a
CC(2): acc system	C1	E2		ok	ok	ok	ok	ok	ok	ok

Result explanation: For the processing of payments and reconciliation of accounts between the accounting and bank transaction services, system accounts are used. In addition, also a shared user account was found; it was used by accountants, which is not in accordance with the requirements (PiSys rated nok at PP2).

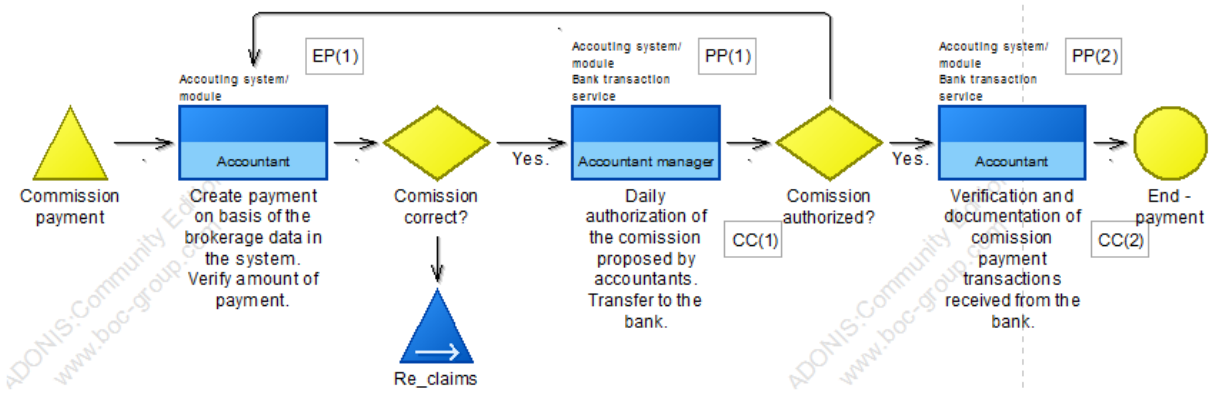


Figure A-65 Accounting commission payment process

Table A-44: Accounting commission payments results company 3

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): acc sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): acc sys	AC2	A2	D3	ok	ok	ok	ok	nok	ok	ok
PP(2): acc sys	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): bank service	C1	E2		ok	ok	ok	ok	ok	ok	ok
CC(1): bank service	C1	E2		ok	ok	ok	ok	ok	ok	ok

Result explanation: For the processing of payments and reconciliation of accounts between the accounting and bank transaction services, system accounts are used. In addition, also a shared user account was found; it was used by accountants, which is not in accordance with the requirements (PiSys rated nok at PP1).

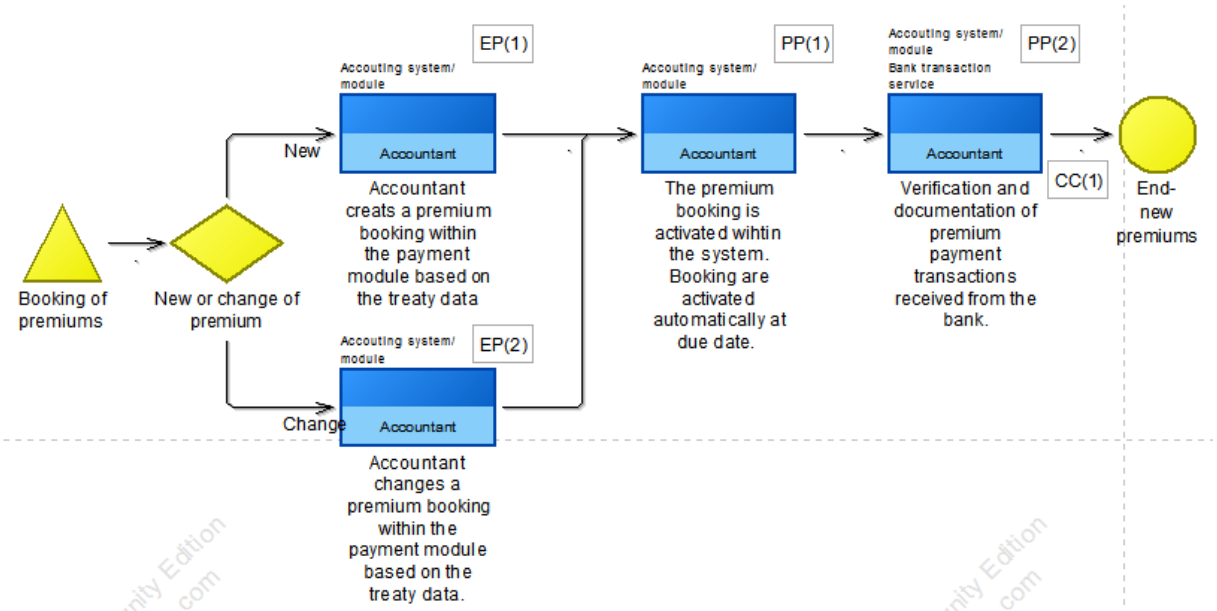


Figure A-66 Accounting booking of new and changes in premiums

Table A-45: Accounting booking of new and changes in premiums results company 3

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): acc sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
EP(2): acc sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): acc sys	AC2	A2	D1	ok	ok	ok	ok	ok	ok	ok
PP(2): acc sys	AC2	A3	D4	ok	ok	ok	ok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): bank service	C1	E2		ok	ok	ok	ok	ok	ok	ok

Result explanation: No issues found.

Underwriting process evaluation (Company 3)

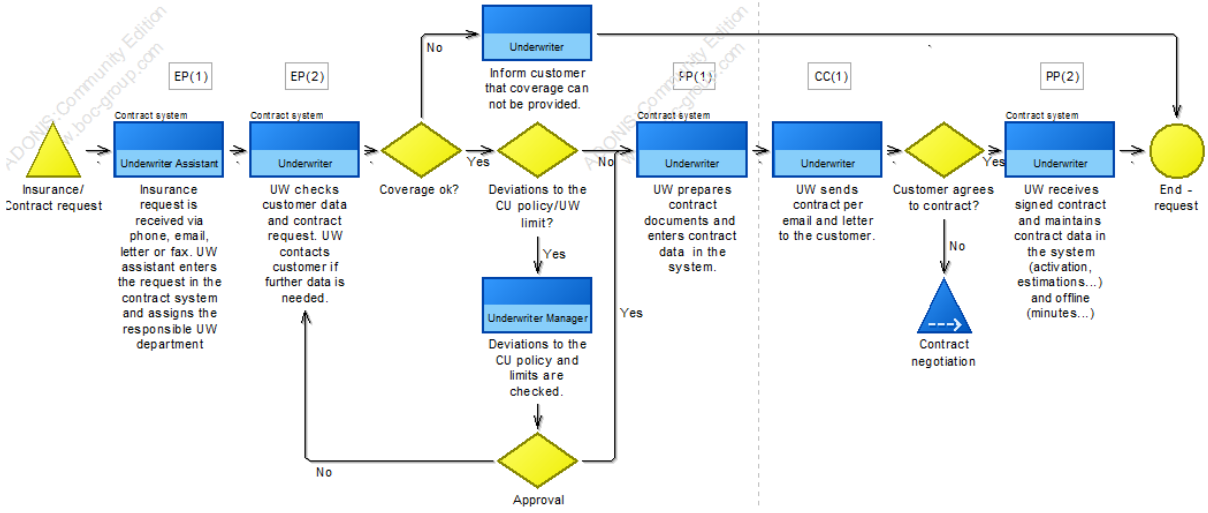


Figure A-67 Insurance/contract request process

Table A-46: Underwriting contract request and offer results company 3

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): contract sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
EP(2): contract sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): contract sys	AC2	A3	D0	nok	ok	ok	nok	nok	ok	ok
PP(2): contract sys	AC2	A3	D3	ok	ok	ok	ok	ok	nok	ok
CC	**A**	**E**					**CC**			
CC(1): customer	C1	E1		nok	nok	ok	ok	ok	ok	ok

Result explanation: There is no system-supported authorisation process for the release of quotations at PP2 (Org rated as nok). Inaccurate expected loss ratio data is used at PP1 (thus the PP1 processing result of nok). Spreadsheets are used for the calculation of premiums, which are not secured and verified at PP1 (PiSys nok). The local actuarial model used at PP1 for premium calculation is not in line with the central model and guidelines. The encryption issue at CC1 was

accepted, as a letter is deemed as secure. Therefore the CC1 processing result was set to ok.

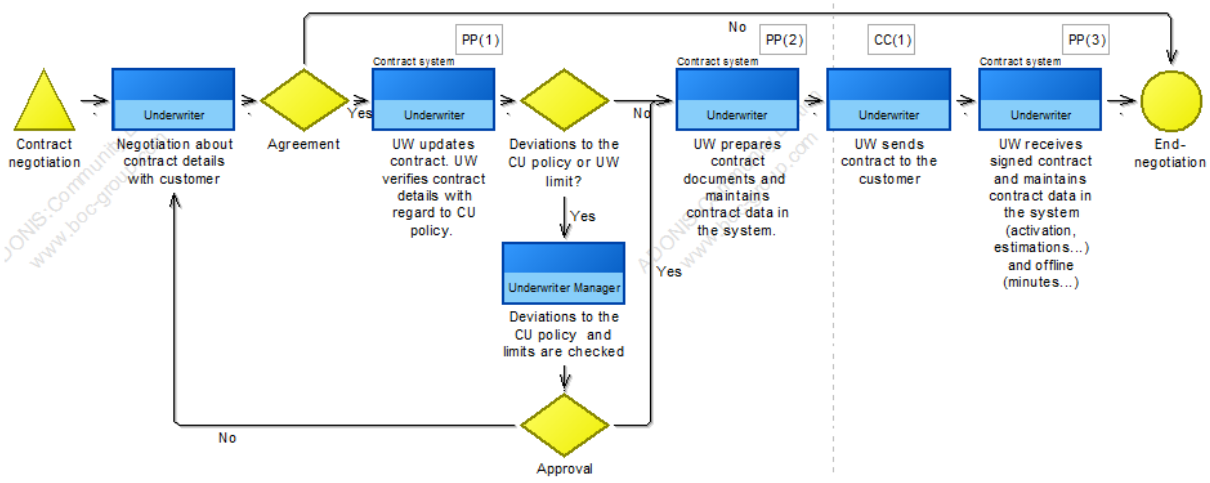


Figure A-68 Contract negotiation process

Table A-47: Underwriting contract negotiation results company 3

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): none	n/a	n/a	n/a	n/a		n/a	n/a	n/a	n/a	n/a
PP							**PP**			
PP(1): contract sys	AC2	A4	D1	nok	ok	ok	nok	ok	ok	ok
PP(2): contract sys	AC2	A4	D1	nok	ok	ok	nok	nok	ok	ok
PP(3): contract sys	AC2	A4	D1	nok	ok	ok	nok	ok	ok	ok
CC	**A**	**E**					**CC**			
CC(1): customer	C1	E1		nok	nok	ok	ok	ok	ok	ok

Result explanation: Inaccurate expected loss ratio data is used at PP2 (PiSys reated nok). Furthermore, full control in the system and the missing verification of data (only manual) leads to non-adherence of integrity security objective (PP1 to PP3 processing result nok). The encryption issue at CC1 was accepted, as a letter is deemed as secure. Therefore the CC1 processing result was set to ok.

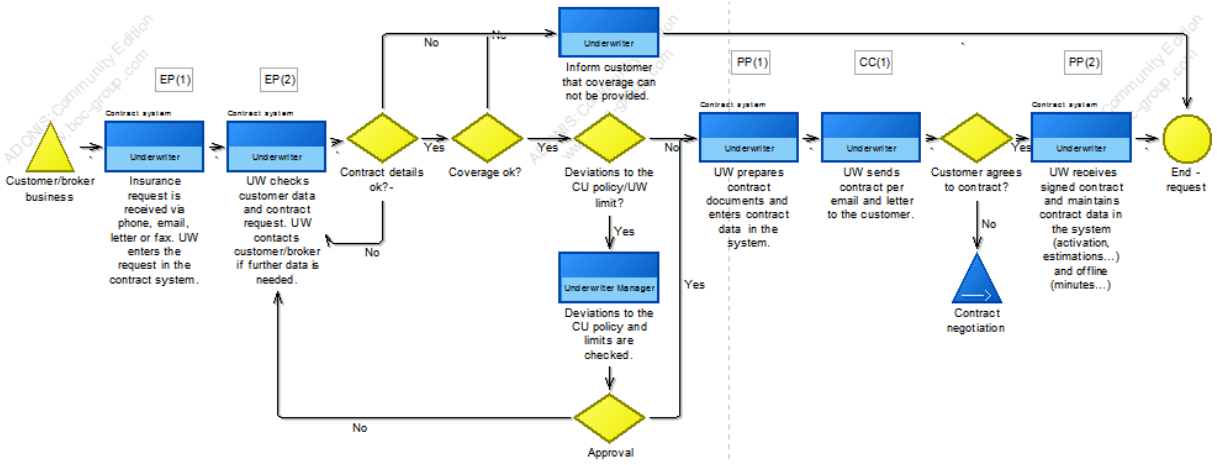


Figure A-69 Customer and broker business process

Table A-48: Underwriting customer and broker business results company 3

Entry, Process and Communication points rating				Processing (SO) Assessment			Processing Result	Container (SR) Assessment		
EP	**AC**	**A**	**D**	**I**	**C**	**A**	**EP**	**PiSys**	**Org**	**Phy**
EP(1): contract sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
EP(1): contract sys	AC2	A3	D1	ok		ok	ok	ok	ok	ok
PP							**PP**			
PP(1): contract sys	AC2	A3	D0	nok	ok	ok	nok	nok	nok	ok
PP(2): contract sys	AC2	A3	D3	ok	ok	ok	ok	ok	nok	ok
CC	**A**	**E**					**CC**			
CC(1): customer	C1	E1		nok	nok	ok	nok	n/a	nok	ok

Result explanation: There is no system-supported authorisation process for the release of quotations at PP2 (Org nok). Inaccurate expected loss ratio data is used at PP1, which is not verified further (PP1 processing result nok). Spreadsheets are used for the calculation of premiums; these are not secured and verified at PP1 (PiSys nok). The local actuarial model used at PP1 (Org nok) for premium calculation is not in line with the central model and guidelines. The encryption issue at CC1 was accepted, as a letter is deemed as secure. However, in further interviews, Underwriters confirmed that from time to time, both claims and profit and loss data is exchanged with brokers via the internet. No encryption is applied to these data (CC1 Org rated nok and CC1 processing result left as nok).

Security process evaluation (Company 3)

Table A-49: Security process evaluation results

IT process name	Sub-process name or Control Objective	Evaluated	Affected Data	Identified issue
Service Strategy	Service Portfolio Management	no		
	Financial Management	no		
Service Design	Service Catalogue Management	no		
	Service Level Management	no		
	Risk Management	no		
	Capacity Management	yes	all	None
	Availability Management	yes	all	None
	IT Service Continuity Management	yes	all	The BCM and DR documentation is insufficient, it does not contain all applications
	IT Security Management	yes	all	Missing security patches were found as identified in the patch report.The security incident process was not followed in the case a virus was spotted or when equipment was lost
	Compliance Management	no		
	IT Architecture Management	no		
	Supplier Management	no		
Service Transition	Change Management	yes	all	None
	Project Management	no		
	Release and Deployment Management	no		
	Service Validation and Test	no		
	Application Development and Test	no		
	Service Asset and Configuration Management	yes	all	In general, there is no configuration management database established
	Knowledge Management	no		
Service Operation	Event Management	no		
	Incident Management	no		
	Request Fulfilment	no		
	Access Management	yes	all	An user access list (who has access to what data) for the different applications and folders could not be provided immediately
	Problem Management	no		
	IT Operations Management	yes	all	None
	IT Facilities Management	yes	all	During the walkthrough unsecured information was found on desks or in unlocked lockers

Continual Service Improvement	Service Evaluation	no		
	Process evaluation	no		
	Definition of process improvements	no		
	Tracking of improvements	no		

Table A-50: Result presentation company 3

Processes/Issues – Information asset	Claims data	Accounting data	Underwriting data	Significance
Claims processes				
There is no authorisation activity in the claims process. (Claims payment process)	X			Medium
Underwriting processes				
Review and release of quotations in the system were not in line. There is no system-supported authorisation process. (Underwriting contract request/ offer and customer/broker business)			X	High
Inaccurate data from systems are used in the expected loss ratio studies. (Underwriting contract request/ offer and customer/broker business and contract negotiation)			X	High
Inappropriate use of spreadsheets for the calculation of premiums. (Underwriting contract request/ offer and customer/broker business)			X	High
Local actuary model not aligned with central model. (Underwriting contract request/ offer and customer/broker business)			X	Medium
IT security processes				
Shared accounts were found, e.g. for the bank service (accounting payment processes)		X		Medium
The security patch report revealed that some patches were missing.	X	X	X	Medium
The business continuity and disaster recovery documentation was missing applications.	X	X	X	Medium
IT was not able to provide user access lists for applications.				Low
Paper documents were stored in unsecured lockers.	X	X	X	Low
It was found that a configuration management system did not exist.				Medium
In a few cases where viruses were identified as well as equipment was lost; the security incident process was not followed.				Medium
Confidential information was exchanged via the internet (Underwriting customer and broker business process).	X	X	X	Medium

v. ARA Company 1 results

Scope: The scope of the assessment was to assess compliance with internal guidelines and regulations, the adequacy and transparency of documentation, as well as the expediency, effectiveness, efficiency and security of the core IT processes. The results were verified by random samples, security scanning and by a “walkthrough” of the premises.

Subjects of evaluation: The subjects of evaluation were critical business systems, infrastructure systems, and IT operation processes. Furthermore, the security awareness of users was examined, as well as any existent documentation regarding the fulfilment of IT processes.

Table A-51: Questionnaire with results of company 1 assessor 1

1.	**General IS awareness**
1.1	User education and training Subject: Training organisation, program and performance
1.2	User awareness Subject: Users’ awareness regarding information security
	Employees interviewed were not aware of current security threats and the content of the local information security policy, or even where to find it.
	In the Claims department, sensitive data is handled which is in most cases handled in a secure manner. There are “Compactus”-units (archives) which the last leaving employee has to lock. One Compactus unit was not locked after office hours. *A "secure desk policy" is in place, which means confidential documents have to be locked in drawers after office hours. As seen on the walkthrough, the policy is not always adhered to as some data was lying on the desk, in open cabinets or on the printer after office hours.*
2.	**IT management and IS compliance**
2.1	IT processes, organisation and relationships Subject: Organisation chart, services and their descriptions
2.2	Regulatory Compliance Subject: National or international tax, data or encryption regulations
2.3	Data - Data ownership, Classification and Handling Subject: Regulations and measures for classification, storage and deletion of data
3.	**Systems security and operation management**
3.1	Service Desk, incidents and problems Subject: Help desk activities, performance and service, problem management
3.2	Configuration management - Hard-/Software Subject: Software releases, inventory, configuration and license management
3.3	IT investment, performance and capacity Subject: IT cost monitoring and budget planning processes
3.4	Systems security - Infrastructure Audit subject: Infrastructure configuration and administration
	Active directory naming conventions, structure and group conventions were not adhered to.

	Unused and active administrative accounts were found in some of the AD groups.
	The local testing was performed on the firewall. The test revealed that websites such as Gmail are not blocked, causing a security threat for the company.
	While patch levels across workstations were generally very good, patch levels on servers were not. Most servers are missing on average 40 patches, e.g. the server for the accounting system. Many of these missing patches are rated "High" at the Security Patch Database.
3.5	Systems security - desktop Subject: Desk policy, configuration and administration
3.6	Solutions and changes - software configuration Subject: Program configuration, controls and documentation
	There is secure processing between the accounting and the online banking software. Furthermore, there is a chart of systems available showing applications and their interfaces. We spotted that some financial data and payments are processed by sending information via email to the bank. This communication channel is insecure.
4.	**Physical and logical access**
4.1	User and Access Rights Management Subject: User access rights and processes
	Permissions in the business applications were mainly set properly. There was only one system identified - the claims system - where claims specialist users have unrestricted access to data.
4.2	Site design and access Subject: Physical access and maintenance of security measures
5.	**Backup, disaster recovery and BCM**
5.1	Data - backup Subject: Data backup and restore processes and documentation
5.2	Continuous service - recovery and planning Subject: Disaster and contingency procedures and documentation
	There is a disaster recovery plan and a business continuity plan in place, however important details (like the restore order) are missing. Furthermore, the responsible IT person is not familiar with the concept and its detail; the plan is not tested.
6.	**Software development and projects**
6.1	Project management Subject: Project management, plan and controlling
6.2	Software development Subject: Specifications, change management, test, data migration and conversion and release

Table A-52: Company 1 results assessor 1

Company 1 Results – Assessor 1	Significance
1. Permissions in the claims system are not properly set.	Medium
2. The transmission of data between the bank and the company is insecure.	Medium
3. Most servers are missing several patches.	High
4. Some websites rated as insecure are not blocked at the firewall.	Low
5. Unused and active administrative accounts in MS Active Directory.	Low
6. Employees are not aware about IS threats and policies.	Low
7. The disaster recovery and business continuity documentation misses important information and was not tested.	Medium
8. In the walkthrough, documents were found not stored securely.	Low

Table A-53: Questionnaire with results of company 1 assessor 2

1.	**General IS awareness**
1.1	User education and training Subject: Training organisation, program and performance
1.2	User awareness Subject: Users' awareness regarding information security
	A policy is in place to keep confidential documents locked in drawers after office hours. Interviewed people on both management and operational levels showed differing sensitiveness about the confidentiality requirements of life/medical information. *As seen on the walkthrough after business-hours, the policy is not always adhered to. We found claims data lying on the desk and in open lockers; audit reports were left on the table. Confidential strategic planning information was easily accessible in open cabinets. We found USB sticks lying on employees' desks.*
	The ISC conducted an awareness and security training program to upper management and new employees. Other employees received only an awareness presentation by email. The security awareness training was not mandatory and the attendance was not tracked. Interviews showed that people without face-to-face training had little knowledge about IS threats.
2.	**IT management and IS compliance**
2.1	IT processes, organisation and relationships Subject: Organisation chart, services and their descriptions
2.2	Regulatory Compliance Subject: National or international tax, data or encryption regulations
2.3	Data - Data ownership, Classification and Handling Subject: Regulations and measures for classification, storage and deletion of data
3.	**Systems security and operation management**
3.1	Service desk, incidents and problems Subject: Helpdesk activities, performance and service, Problem management
3.2	Configuration management - Hard-/Software Subject: Software releases, inventory, configuration and license management
3.3	IT investment, performance and capacity Subject: IT cost monitoring and budget planning processes
3.4	Systems security - Infrastructure Audit subject: Infrastructure configuration and administration
	A significant number of servers are behind on a very large number of security patches. Many of these are rated "High" in the Security Patch Database.
	Webmail sites like Hotmail, Gmail, Yahoo are accessible through the proxy server which is not allowed by Group policy.
3.5	Systems security - desktop Subject: Desk Policy, configuration and administration
3.6	Solutions and changes - software configuration Subject: Program configuration, controls and documentation
	In the claims system, there were still users which left the company. In addition, the claims specialists' role, assigned to several users, had unrestricted user rights in the claims system.
	The banking and accounting application use a secure https data transmission. However, there is financial data and payroll master-data that are exchanged via email to the bank.
4.	**Physical and logical access**
4.1	User and Access Rights Management Subject: User access rights and processes
4.2	Site design and access Subject: Physical access and maintenance of security measures
5.	**Backup, disaster recovery and BCM**
5.1	Data - backup

	Subject: Data backup and restore processes and documentation
5.2	Continuous service - recovery and planning Subject: Disaster and contingency procedures and documentation
	Procedures for backup, disaster recovery as well as a business continuity were not properly defined and documented. A business continuity test involving business departments is outstanding.
6.	**Software development and projects**
6.1	Project management Subject: Project management, plan and controlling
6.2	Software development Subject: Specifications, change management, test, data migration and conversion and release

Table A-54: Company 1 results assessor 2

Company 1 Results – Assessor 2	Significance
1. Unrestricted user rights in the claims system.	Medium
2. Insecure data transmission via email.	Medium
3. Security patches are missing on several servers.	High
4. Websites are not blocked at the proxy server.	Medium
5. Staff had little knowledge about IS threats.	Low
6. No appropriate documentation for disaster recovery and business continuity.	Medium
7. Confidential information was not securely stored, e.g. Claims data.	Low

Consolidated results

Table A-55: Company 1 consolidated results

Company 1 Results	Assessor 1	Assessor 2	Significance
1. The claims specialist has unrestricted access in the claims system.	Yes	Yes	Medium
2. Data transfer between the bank and the company is insecure as only a weak encryption is used.	Yes	Yes	Medium
3. The operating systems e.g. of the accounting system misses several patches.	Yes	Yes	High
4. The firewall is not properly configured; websites are not blocked.	Yes	Yes	Medium
5. Unused and active administrative accounts in MS Active Directory.	Yes	No	Low
6. Staff are not aware about IS threats.	Yes	Yes	Low
7. There is no appropriate disaster recovery and business continuity documentation.	Yes	Yes	Medium
8. Documents/information were not securely stored e.g. in the Claims Department.	Yes	Yes	Low

vi. ARA Company 2 results

Scope: The scope of the assessment was to assess compliance with internal guidelines and regulations, the adequacy and transparency of documentation, as well as the expediency, effectiveness, efficiency and security of the core IT processes. The results were verified by random samples, security scanning and by a "walkthrough" of the premises.

Subjects of evaluation: The subjects of evaluation were critical business systems, infrastructure systems and IT operation processes. Furthermore, the security awareness of users was examined, as well as any existent documentation regarding the fulfilment of IT processes.

Table A-56: Questionnaire with results of company 2

1.	**General IS awareness**
1.1	User education and training Subject: Training organisation, program and performance
1.2	User awareness Subject: Users' awareness regarding information security
	During the walkthrough, we found not properly locked notebooks, confidential life claim data on desks after business hours, and an unlocked secure paper bin.
2.	**IT management and IS compliance**
2.1	IT processes, organisation and relationships Subject: Organisation chart, services and their descriptions
2.2	Regulatory Compliance Subject: National or international tax, data or encryption regulations
2.3	Data - Data ownership, Classification and Handling Subject: Regulations and measures for classification, storage and deletion of data
	A policy/list for data/system ownership from a business point of view was non-existent, delineating responsibilities for data/systems. The business managers of the departments had no current list of employees with access to their department applications or folders. Data owners are not aware of their responsibilities.
3.	**Systems security and operation management**
3.1	Service Desk, incidents and problems Subject: Help desk activities, performance and service, problem management
3.2	Configuration management - Hard-/Software Subject: Software releases, inventory, configuration and license management
3.3	IT investment, performance and capacity Subject: IT cost monitoring and budget planning processes
3.4	Systems security - Infrastructure Audit subject: Infrastructure configuration and administration
	There is an Internet PC used by both IT staff and business staff for miscellaneous browsing purposes. The VPN connection details were found on the internet PC used by IT; as also,

	corporate data was found saved to the desktop of this computer. IT uses the VPN connection for remote support purposes that does not require dual-factor authentication.
	We found that the "daily checklist" listing activities and processes to verify each day was not filled out correctly or consistently, or at all in some cases. Additionally, references to documents were not up-to-date. The checklist is used to verify that all tasks for IT infrastructure operation has been performed successfully and certified as complete.
	DBA activities are not logged (via audit logging) when they logon and perform any changes to systems used by the business. There is also a single DBA user account that does not follow the naming conventions of other DBA user accounts.
3.5	Systems security - desktop Subject: Desk policy, configuration and administration
3.6	Solutions and changes - software configuration Subject: Program configuration, controls and documentation
4.	**Physical and logical access**
4.1	User and Access Rights Management Subject: User access rights and processes
	Access rights revocation or adjustment does not routinely occur when users move between departments or job functions, and does not follow a defined process. Managers may communicate such access changes to the helpdesk or corporate systems; however, they may just as easily forget or ignore sending such notifications. Access rights for applications are not revoked properly, as, for example, in the HR application.
	We found several administrative accounts in Active Directory that should not be active any longer. In addition, some of these users also had an active DBA account.
	The entity has described the process as one to request, approve software and hardware installations. The data owner or the management has to approve the access request or installations. However, approvals were not always available and it was not mandatory that the process was followed. System access was provided not following the defined process.
4.2	Site design and access Subject: Physical access and maintenance of security measures
5.	**Backup, disaster recovery and BCM**
5.1	Data - backup Subject: Data backup and restore processes and documentation
5.2	Continuous service - recovery and planning Subject: Disaster and contingency procedures and documentation
	Dependencies and the order of the recovery of systems were not specified and updated. In case of an incident, the recovery of systems might fail as the dependencies and restore order are not known.
	The Business Contingency Planning (BCP) documentation describes common scenarios, and most critical systems have been identified However, the BCP has never been tested partially or completely. Furthermore, batteries used are regularly maintained but there was no power shutdown test at the disaster recovery site.
6.	**Software development and projects**
6.1	Project management Subject: Project management, plan and controlling
6.2	Software development Subject: Specifications, change management, test, data migration and conversion and release

Table A-57: Company 2 results

Company 2 Results	Significance
1. Weak VPN connection used by IT staff.	Medium
2. No updated disaster recovery plan.	Medium

3. No testing of the BCM/DR activities.	Medium
4. System access approval process not adequate.	Medium
5. Daily data centre operations procedure not adhered to.	Medium
6. Unused and active administrative accounts in MS Active Directory.	Low
7. Data owner not aware of responsibilities.	Low
8. Unused and active accounts in the HR application.	Medium
9. Paper documents were not securely stored.	Low
10. No audit trail logging activated on database level.	High

vii. ARA Company 3 results

Scope: The scope of the assessment was to assess compliance with internal guidelines and regulations, the adequacy and transparency of documentation, as well as the expediency, effectiveness, efficiency and security of the core IT processes. The results were verified by random samples, security scanning and by a "walkthrough" of the premises.

Subjects of evaluation: The subjects of evaluation were critical business systems, infrastructure systems and IT operation processes. Furthermore, the security awareness of users was examined, as well as any existent documentation regarding the fulfilment of IT processes.

Table A-58: Questionnaire with results of company 3

1.	**General IS awareness**
1.1	User education and training Subject: Training organisation, program and performance
1.2	User awareness Subject: Users' awareness regarding information security
	During our walkthrough we found: confidential information (claims reports with personal data) on desks, at the photocopier as well as in unlocked cabinets.
2.	**IT management and IS compliance**
2.1	IT processes, organisation and relationships Subject: Organisation chart, services and their descriptions
2.2	Regulatory Compliance Subject: National or international tax, data or encryption regulations
2.3	Data - Data ownership, Classification and Handling Subject: Regulations and measures for classification, storage and deletion of data
3.	**Systems security and operation management**

3.1	Service Desk, incidents and problems Subject: Help desk activities, performance and service, Problem management
	A laptop was lost. Its hard disk was not encrypted, and this incident was not reported immediately.
3.2	Configuration management - Hard-/Software Subject: Software releases, inventory, configuration and license management
	An overview of applications used was existent; it clearly showed the interaction with other applications and their interfaces. However, an overview of configuration, the quantity and the description of software and hardware was not existent. Hardware and software is configured by the administrators, but not in a structured way, and the configuration is not documented.
3.3	IT investment, performance and capacity Subject: IT cost monitoring and budget planning processes
3.4	Systems security - Infrastructure Audit subject: Infrastructure configuration and administration
	A number of systems have been identified as missing patches by the security monitoring scan.
	Some of the AD user groups used for granting access to folders and applications contained unused and active administrative accounts. Some of these administrative user accounts were MS-standard administrative accounts. Furthermore, the Domain Admin group contained regular user accounts; this is not allowed by the AD administration policy.
3.5	Systems security - desktop Subject: Desk policy, configuration and administration
3.6	Solutions and changes - software configuration Subject: Program configuration, controls and documentation
4.	**Physical and logical access**
4.1	User and Access Rights Management Subject: User access rights and processes
	Application owners are fairly well identified. However, application owners do not receive any reports or verification processes governing application access. Therefore, access right revocation or adjustment does not routinely occur.
	HR department uploads payment files to a bank. A user account and password is necessary to access that function. A shared user account/password is used. A single person can do this without a second authorisation. The upload files are not encrypted and can be modified by a simple text editor before the upload.
	In a user list of the HR application, we found active user accounts of terminated users, as well as generic accounts. Furthermore, the generic accounts had simple and plaintext readable passwords.
4.2	Site design and access Subject: Physical access and maintenance of security measures
5.	**Backup, disaster recovery and BCM**
5.1	Data - backup Subject: Data backup and restore processes and documentation
	Authenticated users can connect and modify the configuration of the disk arrays, part of the virtual tape backup system, without authentication.
5.2	Continuous service - recovery and planning Subject: Disaster and contingency procedures and documentation
	There is a draft BCM plan existing, but not approved and in operation yet. The BCM plan is missing some of the critical applications as identified by the business owners.
6.	**Software development and projects**
6.1	Project management Subject: Project management, plan and controlling
6.2	Software development Subject: Specifications, change management, test, data migration and conversion and release

Table A-59: Company 3 results

Company 3 Results	Significance
1. Shared account used for the online banking system.	High
2. The operating systems for various servers are missing several patches.	High
3. No business continuity and disaster recovery plan in place.	Medium
4. Unused and active administrative accounts in MS Active Directory.	Medium
5. No user access lists for local applications.	Low
6. Unused and active accounts in the HR application.	Medium
7. Paper documents were not securely stored.	Low
8. No configuration management existent.	Medium
9. Weak passwords for the backup recovery tool.	Medium
10. The security incident process was not adhered to.	Medium

A.5. Security objective ratings – Rule set

Security Objective		Integrity			Confidentiality			Availability			
		Level 1	Level 2	Level 3	Level 1	Level 2	Level 3		Level 3	Level 2	Level 1
Security Concept											
Access Control								**Performance**			
unauthenticated user	AC0	EP and >= D2 PP	EP and D4 PP and <= A1	EP failed PP and <= A1	PP and <= A2	PP failed	PP failed	Never met	P1	Failed	Failed	Failed
internal user	AC1	EP and >= D1 PP	EP and >= D2 PP and <= A2	EP failed PP and <= A1	PP and <= A3	PP and <= A3	PP failed	Partially met	P2	Failed	Failed	Failed
authenticated user	AC2	EP and >= D1 PP	EP and >= D1 PP and A3 and >=D1	EP and >= D2 PP and (A3 or A4 and D4)	PP	PP	PP and <= A3	Partially not met	P3	Failed	P3 and M2 or M3 or M4	P3 and M1or M2 or M3 or M4
System user	AC3	EP PP	EP PP	EP PP	PP	PP	PP	Always met	P4	P4 and M3 or M4	P4 and M2 or M3 or M4	P4 and M1 or M2 or M3 or M4
Authorisation								**Measures**				
none	A0	PP	PP	PP	PP	PP failed	PP failed	none	M0	Failed	Failed	Failed
Read	A1	PP	PP	PP	PP	PP and >= AC1	PP and >= AC2	Cold standby	M1	Failed	Failed	M1 and P3 or P4
Execute/process	A2	PP	PP >= AC1	PP and >= AC2	PP	PP and >= AC1	PP and >= AC2	Hot standby	M2	Failed	M2 and P3 or P4	M2 and P3 or P4
Write/update	A3	PP and >= D3	PP and D4 or AC2 and >= D1 or AC3	PP and (AC2 and D4) or AC 3	PP and >= AC1	PP and >= AC1	PP and >= AC2	Redundancy	M3	M3 and P4	M3 and P3 or P4	M3 and P3 or P4

Full control	A4	PP and >= D3	PP and D4 or (AC2 and D2) or AC 3	PP and (AC2 and D4) or AC 3	PP and >= AC2	PP and >= AC2	PP and >= AC2	Cluster	M4	M4 and P4	M4 and P3 or P4	M4 and P3 or P4
Data validation												
None	D0	EP failed	EP failed	EP failed	n/a	n/a	n/a					
Manual	D1	EP and >= AC1	EP and AC2	EP failed	n/a	n/a	n/a					
Downstream resonableness validation	D2	EP	EP and >= AC1	EP and AC2	n/a	n/a	n/a					
Value verification	D3	EP	EP and AC2	EP and AC2	n/a	n/a	n/a					
Value verification and completeness	D4	EP	EP	EP and AC2	n/a	n/a	n/a					
Communication												
External unauthenticated partner	C0	CC and >= E1	CC failed	CC failed	CC and >=E1	CC and >= E2	CC failed					
External authenticated partner	C1	CC	CC and >= E2	CC and E3	CC and >=E1	CC and >= E2	CC and E3					
Internal network partner	C2	CC	CC	CC and >= E2	CC	CC	CC and >= E2					
Internal authenticated partner	C3	CC	CC	CC	CC	CC	CC					
Encryption												
none	E0	CC failed	CC failed	CC failed	CC and >=C2	CC failed	CC failed					
weak encryption	E1	CC	CC failed	CC failed	CC	CC failed	CC failed					
Standard encryption	E2	CC	CC	CC failed	CC	CC	CC failed					
strong encryption	E3	CC	CC	CC	CC	CC	CC					

A.6. Security objective assessment with Prolog

In the following the (SWI-) Prolog (available at http://www.swi-prolog.org/) program used for the security objective assessment is described. A rule base was defined that determines whether the security objective is adhered to as facts and rules in Prolog. For each security rating with regard to the process points rules are defined with regard to the assessment criteria's that have to be adhered to. If one likes to determine whether the security rating – confidentiality, integrity and availability - for a EP, PP, CC process point complies with the rules defined for confidentiality, integrity and availability with regard to the assessment criteria's – access control, authorisation, data validation, encryption, communication, availability level and measures - one has to start the programm by `assess.` providing the requested information.

The program consists of three main parts – the facts which represent single conditions for security objectives and process points, the assessment rule for security objectives and process points and the query interface to request the information needed for the assessment from the user.

1. Query interface

The program starts with `assess.` by asking for the security objective (`X` = confidentiality, integrity or availability) and rating (`Lev` = level 1 to 3). Next the process point type (`Pp` = ep, pp or cc) is asked by the rule `so(X,Lev)` and dependent of the security objective the rule `integrity(Pp, Lev)`, `confidentiality(Pp, Lev)` or `availability(Lev)` called. At `integrity(Pp, Lev)` and `confidentiality(Pp, Lev)` the EPs and PPs security functions ratings are asked for access control (`Ac` = ac0 to ac3),

authorisation (A = a1 to a4) and data validation (D = d1 to d4). For CCs only the ratings for encryption (E = e0 to e3) and communication (C = c0 to c3) are asked. At availability(Lev) the performance (P = p1 to p4) and measures (M = m1 to m4) rating of systems of an EP, PP and CC is asked. The input has to be provided for each EP, PP and CC subsequently. The input of a security function can be omitted if not available (e.g. by '[]') or asked to be resolved by Prolog by using a variable (e.g. 'Result'). After then the corresponding assessment rules for availability, integrity or confidentiality with regard to the process point type are called.

2. Assessment rules

The assessment rules are called after the user specified the security functions for an EP, PP or CC to evalaute the adherence of the security objective.

Integrity is evaluated for EPs, PPs and CCs. The following rules were defined:

```
integrity_EP(Lev,Ac,D):-
(ep_int_data(Lev,D);ep_int_access(Lev,Ac);ep_int_data_access(
Lev,Ac,D)).
```

The EP security function ratings are checked whether the ratings for data validation (ep_int_data) or access control (ep_int_access) or a combination of both (ep_int_data_access) correspond with the facts defined for the specified integrity level (Lev).

```
integrity_PP(Lev,Ac,A,D):-(pp_int_access(Lev,Ac);
pp_int_auth(Lev,A); pp_int_access_auth(Lev,Ac,A,D)).
```

The PP security function ratings are checked whether the ratings for access control (pp_int_access) or authorisation (pp_int_auth) or a combination of all three (pp_int_access_auth) including data validation correspond with the facts defined for the specified integrity level (Lev).

```
integrity_CC(Lev,C,E):-
(cc_int_com(Lev,C);cc_int_enc(Lev,E);cc_int_com_enc(Lev,C,E))
,not(cc_int_com_enc_no(Lev,C,E)).
```

The CC security function ratings are checked whether the ratings for communication (cc_int_com) or encryption (cc_int_enc) or a combination of both (cc_int_com_enc) correspond with the facts defined for the specified integrity level (Lev). In addition, it is checked that some security function rating do not become true with cc_int_com_enc_no(Lev,C,E).

Confidentiality is only evaluated at PPs and CCs as for EP no confidentiality requirements from a processing view have to be adhered to. The following rules were defined:

```
confidentiality_PP(Lev,Ac,A):-
(pp_conf_access(Lev,Ac);pp_conf_auth(Lev,A);pp_conf_access_au
th(Lev,Ac,A)).
```

The PP security function ratings are checked whether the ratings for access control (pp_conf_access) or authorisation (pp_conf_auth) or a combination of both (pp_conf_access_auth) correspond with the facts defined for the specified confidentiality level (Lev).

```
confidentiality_CC(Lev,C,E):-
(cc_conf_com(Lev,C);cc_conf_enc(Lev,E);cc_conf_com_enc(Lev,C,
E)),not(cc_conf_com_enc_no(Lev,C,E)).
```

The CC security function ratings are checked whether the ratings for communication (cc_conf_com) or encryption (cc_conf_enc) or a combination of both (cc_conf_com_enc) correspond with the facts defined for the specified confidentiality level (Lev). In addition, it is checked that some security function rating do not become true with cc_conf_com_enc_no(Lev,C,E).

Availability is evaluated without distinction of EPs, PPs and CCs and therefore directly by the facts defined. The rule availability_EPPPCC(Lev,P,M) verifies the ratings for performance and measure with regard to the facts defined for an availability level. Lev contains the security objective level and is only used to distinguish between the facts defined for the different security objective levels.

3. Facts

The facts defined describe a true condition for an EP, PP and CC for integrity, confidentiality and availability with regard to the implementation of security functions. The facts are used by the assessment rules to verify whether the statement for an EP,PP or CC is true. The facts were constructed like the following: `Name_of_the_fact(Security objective level, security function ratings)`.The security function rating can be only one argument or more. E.g. `ep_integrity(level1, ac0, d1).` represents a fact with two arguments for integrity level 1.

Prolog program

```
/*Facts for verifying integrity for EP */
ep_int_data(level1,d2).
ep_int_data(level1,d3).
ep_int_data(level1,d4).
ep_int_access(level1,ac3).
ep_int_data_access(level1,ac0,d2).
ep_int_data_access(level1,ac1,d1).
ep_int_data(level2,d4).
ep_int_access(level2,ac3).
ep_int_data_access(level2,ac2,d1).
ep_int_data_access(level2,ac1,d2).
ep_int_data_access(level2,ac2,d2).
ep_int_data_access(level2,ac2,d3).
ep_int_data_access(level2,ac1,d3).
ep_int_access(level3,ac3).
ep_int_data_access(level3,ac2,d2).
ep_int_data_access(level3,ac2,d3).
ep_int_data_access(level3,ac2,d4).
/*Integrity assessment rule for a EP */
integrity_EP(Lev,Ac,D):-
(ep_int_data(Lev,D);ep_int_access(Lev,Ac);ep_int_data_access(Lev,Ac,D)).

/*Facts for verifying integrity for PP */
pp_int_access(level1,ac0).
pp_int_access(level1,ac1).
pp_int_access(level1,ac2).
pp_int_access(level1,ac3).
pp_int_auth(level1,a0).
pp_int_auth(level1,a1).
```

```
pp_int_auth(level1,a2).
pp_int_access_auth(level1,_,a3,d3).
pp_int_access_auth(level1,_,a3,d4).
pp_int_access_auth(level1,_,a4,d3).
pp_int_access_auth(level1,_,a4,d4).
pp_int_access(level2,ac3).
pp_int_auth(level2,a0).
pp_int_auth(level2,a1).
pp_int_access_auth(level2,ac2,a3,d1).
pp_int_access_auth(level2,ac2,a3,d2).
pp_int_access_auth(level2,ac2,a3,d3).
pp_int_access_auth(level2,ac2,a3,d4).
pp_int_access_auth(level2,_,a4,d4).
pp_int_access_auth(level2,ac2,a4,d2).
pp_int_access_auth(level2,ac1,a2,_).
pp_int_access_auth(level2,ac1,a2,_).
pp_int_access_auth(level2,ac2,a2,_).
pp_int_access_auth(level2,ac3,a2,_).
pp_int_access(level3,ac3).
pp_int_auth(level3,a0).
pp_int_auth(level3,a1).
pp_int_access_auth(level3,ac2,a2,_).
pp_int_access_auth(level3,ac2,a3,d4).
pp_int_access_auth(level3,ac2,a4,d4).
/*Integrity assessment rule for a PP.*/
integrity_PP(Lev,Ac,A,D):-(pp_int_access(Lev,Ac); pp_int_auth(Lev,A);
pp_int_access_auth(Lev,Ac,A,D)).

/*Facts for verifying confidentiality for PP */
pp_conf_access(level1,ac2).
pp_conf_access(level1,ac3).
pp_conf_auth(level1,a0).
pp_conf_auth(level1,a1).
pp_conf_auth(level1,a2).
pp_conf_access_auth(level1, ac0, a0).
pp_conf_access_auth(level1, ac1, a3).
pp_conf_access_auth(level1, ac2, a3).
pp_conf_access_auth(level1, ac3, a3).
pp_conf_access_auth(level1, ac2, a4).
pp_conf_access_auth(level1, ac3, a4).
pp_conf_access_auth(level2, ac1, a2).
pp_conf_access(level2,ac2).
pp_conf_access(level2,ac3).
pp_conf_access_auth(level2, ac1, a0).
pp_conf_access_auth(level2, ac1, a1).
pp_conf_access_auth(level2, ac1, a2).
pp_conf_access_auth(level2, ac1, a3).
pp_conf_access(level3,ac3).
pp_conf_access_auth(level3, ac2, a1).
pp_conf_access_auth(level3, ac2, a2).
pp_conf_access_auth(level3,ac2,a3).
```

```
pp_conf_access_auth(level3,ac2,a4).
/*Confidentiality assessment rule for a PP */
confidentiality_PP(Lev,Ac,A):-
(pp_conf_access(Lev,Ac);pp_conf_auth(Lev,A);pp_conf_access_auth(Lev,Ac,A)).

/*Facts for verifying integrity for CC */
cc_int_enc(level1,e1).
cc_int_enc(level1,e2).
cc_int_enc(level1,e3).
cc_int_com(level1,c1).
cc_int_com(level1,c2).
cc_int_com(level1,c3).
cc_int_com_enc_no(level1,c0,e0).
cc_int_enc(level2,e2).
cc_int_enc(level2,e3).
cc_int_com(level2,c2).
cc_int_com(level2,c3).
cc_int_com_enc(level2,c1,e2).
cc_int_com_enc(level2,c1,e3).
cc_int_com_enc_no(level2,c0,e0).
cc_int_com_enc_no(level2,c1,e0).
cc_int_com_enc_no(level2,c1,e1).
cc_int_enc(level3,e3).
cc_int_com(level3,c3).
cc_int_com_enc(level3,c1,e3).
cc_int_com_enc(level3,c2,e2).
cc_int_com_enc(level3,c2,e3).
/*Integrity assessment rule for a CC. Not excludes specific rule combinations */
integrity_CC(Lev,C,E):-
(cc_int_com(Lev,C);cc_int_enc(Lev,E);cc_int_com_enc(Lev,C,E)),not(cc_int_com
_enc_no(Lev,C,E)).

/*Facts for verifying confidentiality for CC */
cc_conf_enc(level1,e1).
cc_conf_enc(level1,e2).
cc_conf_enc(level1,e3).
cc_conf_com(level1,c2).
cc_conf_com(level1,c3).
cc_conf_com_enc(level1,c0,e1).
cc_conf_com_enc(level1,c2,e0).
cc_conf_com_enc(level1,c3,e0).
cc_conf_com_enc(level1,c1,e1).
cc_conf_com_enc_no(level1,c0,e0).
cc_conf_com_enc_no(level1,c1,e0).
cc_conf_enc(level2,e2).
cc_conf_enc(level2,e3).
cc_conf_com(level2,c2).
cc_conf_com(level2,c3).
cc_conf_com_enc(level2,c0,e2).
cc_int_com_enc_no(level2,c1,e1).
cc_conf_com_enc_no(level2,c0,e1).
```

```
cc_conf_com(level3,c3).
cc_conf_enc(level3,e3).
cc_conf_com_enc(level3,c2,e2).
cc_conf_com_enc(level3,c1,e3).
/*Confidentiality assessment rule for a CC. The Not statement excludes some rule combinations */
confidentiality_CC(Lev,C,E):-
(cc_conf_com(Lev,C);cc_conf_enc(Lev,E);cc_conf_com_enc(Lev,C,E)),not(cc_conf_com_enc_no(Lev,C,E)).

/*Facts for verifying availability for EP,PP,CC */
availability_EPPPCC(level3,p4,m3).
availability_EPPPCC(level3,p4,m4).
availability_EPPPCC(level2,p3,m2).
availability_EPPPCC(level2,p3,m3).
availability_EPPPCC(level2,p3,m4).
availability_EPPPCC(level2,p4,m2).
availability_EPPPCC(level2,p4,m3).
availability_EPPPCC(level2,p4,m4).
availability_EPPPCC(level1,p3,m1).
availability_EPPPCC(level1,p3,m2).
availability_EPPPCC(level1,p3,m3).
availability_EPPPCC(level1,p3,m4).
availability_EPPPCC(level1,p4,m1).
availability_EPPPCC(level1,p4,m2).
availability_EPPPCC(level1,p4,m3).
availability_EPPPCC(level1,p4,m4).

/*Start the the assessment and query security objective and the security objective level */
assess:- write('Please type SO integrity, confidentiality,
availability:'),nl,read(X),write('Please type level 1 to 3:'),nl,read(Lev),so(X,Lev).

/* Query process point type*/
so(X,Lev):- ('integrity'=X, write('Please type
ep,pp,cc'),nl,read(Pp),integrity(Pp,Lev));('confidentiality'=X, write('Please type
ep,pp,cc'),nl,read(Pp),confidentiality(Pp,Lev));('availability'=X,availability(Lev)).

/* Query the security function ratings for evaluating integrity for EP or PP or CC*/
integrity(Pp,Lev):- (('ep'=Pp;'pp'=Pp),write('Access rating(ac0-
ac3)?'),nl,read(Ac),write('Authorisation rating (a0-a4)?'),nl,read(A),write('Data
validation rating(d0-
d4)'),nl,read(D),('ep'=Pp,integrity_EP(Lev,Ac,D);'pp'=Pp,integrity_PP(Lev,Ac,A,D)))
;('cc'=Pp,write('Communication rating (c0-c3)'),nl,read(C), write('Encryption rating
(e0-e3)?'),nl,read(E),integrity_CC(Lev,C,E)).

/* Query the security function ratings for evaluating confidentiality for PP or CC */
confidentiality(Pp,Lev):- ('pp'=Pp,write('Access rating(ac0-
ac3)?'),nl,read(Ac),write('Authorisation rating (a0-
a4)?'),nl,read(A),confidentiality_PP(Lev,Ac,A));('cc'=Pp,write('Communication
```

```
rating (c0-c3)'),nl,read(C), write('Encryption rating (e0-
e3)?'),nl,read(E),confidentiality_CC(Lev,C,E)).

/*Query the security functions ratings for evaluating availability */
availability(Lev):- write('Performance rating(p1-p4)?'),nl,read(P), write('Measure
rating(m1-m4)?'),nl,read(M),availability_EPPPCC(Lev,P,M).
```

Glossary

In the following, definitions for terms used in this thesis are provided.

Availability
ensures that resources are accessible and usable on demand by authorised entities (ISO, 2004b).

Confidentiality
ensures that information is not made available to unauthorised entities (ISO, 2005c).

Event
is the occurrence or change of a particular set of circumstances (ISO, 2009a) caused by a threat.

Information security
is the preservation of confidentiality, integrity and availability of information (ISO, 2005c).

Information security risk
is the combination of the probability of an event and its consequence (ISO, 2012), which would result in the violation of security objectives.

Integrity
is the protection of the accuracy and completeness of assets (ISO, 2004b).

Impact
is an adverse change to the level of business objectives achieved (ISO, 2012).

Risk analysis
is the process to comprehend the nature of risk and to determine the level of risk (ISO, 2009a).

Risk assessment
is the overall process of risk identification, risk analysis and risk evaluation (ISO, 2009a).

Risk management
is the application of process and procedures to the activities of identifying, analyzing, evaluating, treating, monitoring, communication and reviewing of risk (adopted from ISO, 2009a).

Risk treatment
is the process of selection and implementation of security functions to modify risk based on security requirements (adopted from ISO, 2009a).

Risk
is the effect of uncertainty on objectives (ISO, 2009a).

Security objective
is a statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions (ISO, 2005f).

Security requirements
are constraints on the functions of the system, where these constraints operationalize one or more security objectives (Haley et al., 2008).

Threat
is a potential cause of an unwanted incident (exercising a vulnerability), which may result in harm to a system or organization (ISO, 2012).

Vulnerability
is a weakness of an asset or control that can be exploited by a threat (ISO, 2012) violating the security objective.

Vulnerability identification errors
are unidentified vulnerabilities or identified vulnerabilities that are not, in fact, vulnerabilities (Taubenberger et al., 2013).

Index

Bibliography

Aagedal, J. y., denBraber, F., Dimitrakos, T., Gran, B. A., Raptis, D. and Stølen, K. (2002), 'Model-based risk assessment to improve enterprise security', *in Proceedings of the Fifth International Enterprise Distributed Object Computing Conference (EDOC 2002)*, pp. 51-62, September 17-20, 2002, Lausanne, Switzerland.

Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003), *Introduction to the OCTAVE approach*, Software Engineering Institute (SEI), Carnegie Mellon University, Pittsburgh, USA, PA 15213-3890.

Albrechtsen, E. (2003), *Security vs safety*, NTNU - Norwegian University of Science and Technology Department of Industrial Economics and Technology Management.

ANSSI (2010*a*), *EBIOS 2010 - Expression of Needs and Identification of Security Objectives*, ANSSI - Agence nationale de la sécurité des systèmes d'information [Online]. Available at http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ (Accessed 30 June 2013).

ANSSI (2010*b*), *Expression des Besoins et Identification des Objectifs de Sécurité - EBIOS - MÉTHODE DE GESTION DES RISQUES*, ANSSI - Agence nationale de la sécurité des systèmes d'information [Online]. Available at http://www.ssi.gouv.fr/en/the-anssi/, (Accessed 30 June 2013).

Arendt, J. (1990), 'Using quantitative risk assessment in the chemical process industry', *Reliability Engineering, System Safety,* 29(1), pp. 133 – 149.

ASNZ (1999), *Australian/New Zealand Standard Risk Management ASNZ 4360:1999*, Australian and New Zealand Standards Comittee.

ASNZ (2004), *Australian/New Zealand Standard Risk Management AS/NZS 4360:2004*, Australian and New Zealand Standards Comittee.

ASNZ (2009), *Australian/New Zealand Standard Risk Management AS/NZS ISO 31000:2009 - Risk Management – Principles and Guideline*, Australian and New Zealand Standards Comittee.

Atluri, V. (2001), 'Security for workflow systems', *Information Security Technical Report,* 6(2), pp. 59–68.

Backes, M., Pfitzmann, B. and Waidner, M. (2003), *Security in Business Process Engineering*. In: van der Aalst, W.M.P., ter Hofstede, A.H.M., Weske, M. (eds.) BPM 2003. LNCS, vol. 2678, pp. 168–183, Springer, Heidelberg (2003).

Backhouse, J. and Dhillon, G. . (1996), 'Structures of responsibility and security of information systems', *European Journal of Information Systems,* 5(1), pp. 2–9.

Badenhorst, K. P. and Eloff, J. H. P. (1994), 'TOPM: a formal approach to the optimization of information technology risk management', *Computers & Security,* 13(5), pp. 411–435.

Bandyopadhyay, K., Mykytyn, P. and Mykytyn, K. (1999), 'A framework for integrated risk management in information technology', *Management Decision,* 37(5), pp. 437–444.

Basel Committee on Banking Supervision (2004*), International convergence of capital measurement and capital standards*, Bank for International Settlements [Online]. Available at http://www.bis.org/publ/bcbs107.htm (Accessed 30 June 2013).

Becker, J., Fischer, R., Janiesch, C. and Scherpbier, H. (2007), 'Optimizing U.S. healthcare processes: A case study in business process management', *in Proceedings of the 13th AMCIS*, Keystone, Colorado.

Beresnevichiene, Y., Pym, D. and Shiu, S. (2010), 'Decision support for systems security investment', *in Network Operations and Management Symposium Workshops (NOMS Wksps)*, 2010 IEEE/IFIP, pp. 118–125.

Bernard, R. (2007), 'Information lifecycle security risk assessment: A tool for closing security gaps', *Computers & Security,* 26, pp. 26–30.

Bishop, M. (2002), *Computer Science: Art and Science*, Addison Wesley 2002.

Bishop, M. (2003), 'What is computer security?', *IEEE Security & Privacy,* pp. 67–69.

BOC (1995), *ADONIS - Business process modeling*, BOC Information Technologies Consulting GmbH [Online]. Available at http://www.boc-group.com, (Accessed 30 June 2013).

Boström, G., Wäyrynen, J., Bodén, M., Beznosov, K. and Kruchten, P. (2006), 'Extending xp practices to support security requirements engineering', *in Proceedings of the 2006 international workshop on Software engineering for secure system (SESS'06)*, May 20–21, 2006, Shanghai, China.

Braber, Hogganvik, Lund, Stølen and Vraalsen (2007), 'Model-based security analysis in seven steps - a guided tour to the coras method', *BT Technology Journal* Vol. 25, No 1, pp. 101–117.

Breu, R. and Innerhofer-Oberperfler, F. (2005), 'Model based business driven it security analysis', *in Proceedings of the Third Symposium on Requirements*

Engineering for Information Security (SREIS'05) held in conjunction with the 13th International Requirements Engineering Conference (RE'05), Paris, France, 2005.

Breu, R., Innerhofer-Oberperfler, F., Mitterer, M., Schabetsberger, T. and Wozak, F. (2008),' Model-based security analyisis of health care networks', *in Proceedings of eHealth2008 - Medical Informatics meets eHealth*, 2008, Vienna.

Brinkley, D. L. and Schell, R. R. (1995), 'Information Security: An Integrated Collection of Essay', *IEEE Computer Society Press, chapter Concepts and Terminology for Computer Security (Essay 2)*, pp. 40–96.

Brodkin, J. (2007), *TJX breach may spur greater adoption of credit card security standards* [Online], Network World. Available at http://www.networkworld.com/news/2007/032907-tjx-breach-adopt-standards.html (Accessed 30 June 2013).

BSI (2008), *BSI-Standard 100-02: IT-Grundschutz Methodology*, Federal Office of Information Security Germany (BSI).

Buyens, K., De Win, B. and Joosen, W. (2007), 'Empirical and statistical analysis of risk analysis-driven techniques for threat management', *in Proceedings of the Second International Conference on Availability, Reliability and Security (ARES '07)*, IEEE Computer Society, Washington, DC, USA, pp. 1034–1041. http://dx.doi.org/10.1109/ARES.2007.78

Campbell, P. L. and Stamp, J. E. (2004), *A classification scheme for risk assessment method*s, Sandia National Laboratories, California, USA, SAND2004-4233.

Caralli, R., Stevens, J., Young, L. and Wilson, W. (2007), *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, Software

Engineering Institute (SEI), Carnegie Mellon University, Pittsburgh, USA, CMU/SEI-2007-TR-012; ESC-TR-2007-012.

Carg, A., Curtis, J. and Harper, H. (2003), 'Quantifying the financial impact of IT security breaches', *Information Management & Computer Security,* 11/2, pp.74–83.

CC (2006), *Common Criteria for Information Technology Security Evaluation*, *Introduction and general model, Version 3.1*, Common Criteria.

CCTA (1987), *CCTA Risk Analysis and Management Method* [Online], Central Computing and Telecommunications Agency (CCTA). Available at http://www.cramm.com/ (Accessed 13 May 2012).

CCTA (2007), *IT Infrastructure Library (ITIL) Version 3*, Central Computing and Telecommunications Agency (CCTA).

Chivers, H. and Fletcher, M. (2005), 'Applying security design analysis to a service-based system', *Software: Practice and Experience,* 35 no. 9, pp. 873–897.

Chung, Y. J., Kim, I., Lee, N., Lee, T. and In, H. P. (2005), 'Security risk vector for quantitative asset assessment', *in Proceedings of Computational Science and Its Applications – ICCSA 2005*, Singapore, May 9-12, 2005, Part II , Springer Berlin / Heidelberg, 2005.

Ciechanowicz, Z. (1997), 'Risk analysis: requirements, conflicts and problems', *Cornputers & Security,* 16(3), pp. 223–232.

CLUSIF (2010), *Mehari 2010 - Risk assessment and treatment Guide*, CLUSIF-Club de la Sécurité de l'Information Français [Online]. Available at http://www.clusif.asso.fr/en/clusif/present/ (Accessed 30 June 2013).

Cockburn, A. (2001), *Writing effective use cases*, Addison-Wesley Longman Publishing Co., Inc. 2001.

Cohen, J. (1960), ‘A coefficient of agreement for nominal scales’, *Educational and Psychological Measurement,* 20, pp. 37–46.

COSO (1994*), Internal Control — Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission [Online]. Available at http://www.coso.org/guidance.htm (Accessed 30 June 2013).

COSO (2004), *Enterprise Risk Management Framework*, Committee of Sponsoring Organizations of the Treadway Commission [Online]. Available at http://www.coso.org/guidance.htm (Accessed 30 June 2013).

Cox, K. and Phalp, K. (2003), ‘Detecting role equivalence&social networks’, *in Pre-Proceedings of the 9th International Workshop on Requirements Engineering – Foundations for Software Quality (REFSQ’03)*, pp. 12–83.

Diebold, F. X., Schuermann, T. and Stroughair, J. D. (1998), ‘Pitfalls and Opportunities in the Use of Extreme Value Theory in Risk Management’, in A.-P. N. Refenes, J.D. Moody and A.N. Burgess (eds.), *Advances in Computational Finance, 3-12*. Amsterdam: Kluwer Academic Publishers. Reprinted in Journal of Risk Finance, 1 (Winter 2000), 30-36.

Dubois, E., Heymans, P., Mayer, N. and Matulevius, R. (2010), ‘A systematic approach to define the domain of information security risk management’, *in International Perspectives on Information Systems Engineering*, pp. 286–306.

Eikebrokk, T. R., Iden, J., Olsen, D. H. and Opdahl, A. L. (2008), ‘Towards a model of process-modelling practice: Quantitative validation and results’, *in Proceedings of the 16th European Conference on Information Systems*, Galway, Ireland, pp. 1608–1619.

ENISA (2006), *Inventory of risk assessment and risk management methods - ENISA ad hoc working group on risk assessment and risk management* [Online], The European Network and Information Security Agency (ENISA). Available at http://www.enisa.org (Accessed 30 June 2013).

ENISA (2008), *2007-2008 ad hoc working group on risk assessment/risk management, determining your organization's information risk assessment and management requirements and selecting appropriate methodologies* [Online], The European Network and Information Security Agency (ENISA). Available at http://www.enisa.europa.eu/act/rm/files/deliverables/determining-your-organization2019s-information-risk-assessment-and-management (Accessed 30 June 2013).

ENISA (2012), *Introduction to Return on Security Investment* [Online], The European Network and Information Security Agency (ENISA). Available at http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment (Accessed 30 June 2013).

ENISA (2013), *Inventory of Risk Management / Risk Assessment Methods* [Online], The European Network and Information Security Agency (ENISA). Available at http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-methods (Accessed 30 June 2013).

Ericson, C. (1999), 'Fault tree analysis – A History', *in Proceedings of the 17th International Systems Safety Conference,* Orlando, FL, 1999.

European Commission (2007), *Proposal for a directive of the European parliament and of the council on the taking-up and pursuit of the business of Insurance and Reinsurance, SOLVENCY II* [Online], European Commission. Available at

http://ec.europa.eu/internal_market/insurance/solvency/latest/index_en.htm, (Accessed 30 June 2013).

European Communities (1991*), Information Technology Security Evaluation Criteria (ITSEC),* Office for Official Publications of the European Communities [Online]. Available at http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf (Accessed 30 June 2013).

Feather, M. S. and Cornford, S. L. (2006), 'Relating risk and reliability predictions to design and development choices', *in Proceedings of the Annual Reliability and Maintainability Symposium (RAMS)*, Newport Beach, CA, 23-26 January, 2006.

Fenz, S. and Ekelhart, A. (2011), 'Verification, Validation, and Evaluation in Information Security Risk Management', *Security Privacy, IEEE,* 9(2), pp. 58 –65.

Firesmith, D. G. (2003), 'Engineering security requirements', *Journal of Object Technology,* 2(1), pp. 53–68.

Frachot, A. and Roncalli, T. (2002), *Mixing internal and external data for managing operational risk* [Online], National Institute of Statistics and Economic Studies (INSEE). Available at http://ssrn.com/abstract=1032525 (Accessed 30 June 2013).

Gerber, M. and von Solms, R. (2001), 'From risk analysis to security requirements', *Computers & Security,* 20, pp. 577–584.

Gerber, M. and von Solms, R. (2008), 'Information security requirements – interpreting the legal aspects', *Computers & Security,* 27(5-6), pp. 124–135.

Gerber, M., von Solms, R. and Overbeek, P. (2001), 'Formalizing information security requirements', *Information Management & Computer Security,* 9(1), pp. 32 – 37.

Giorgini, P. and Mouratidis, H. (2005), ‘Secure tropos: A security-oriented extension of the tropos methodology’, *Journal of Autonomous Agents and Mult-Agent Systems*.

Giunchiglia, F., Mylopoulos, J. and Perini, A. (2002), ‘The tropos software development methodology: Processes, models and diagrams’ *in Proceedings of the AAMAS - The First International Joint Conference on Autonomous Agents and Multi-Agent Systems*, Bologna, Italy — July 15 - 19, 2002.

Guarro, S. (1987), ‘Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management’, *Computers & Security,* 6, pp. 493–504.

Haley, C. B., Laney, R. C. and Nuseibeh, B. (2004), ‘Deriving security requirements from crosscutting threat descriptions’, *in Proceedings of the 3rd international conference on Aspect-oriented software development, AOSD ’04*, ACM, New York, NY, USA, pp. 112–121. http://doi.acm.org/10.1145/976270.976285

Haley, C., Laney, R. and Moffett, J. (2008), ‘Security requirements engineering: A framework for representation and analysis’, *IEEE Transactions on Software Engineering,* 34(1), pp. 133–153.

Halliday, S., Badenhorst, K. and von Solms, R. (1996), ‘A business approach to effective information technology risk analysis and management’, *Information Management &Computer Security,* 4(1), pp. 19–31.

Harmon, P. and Wolf, C. (2008), *The state of business process management* [Online], BPtrends. Available at http://www.bptrends.com/surveys_landing.cfm (Accessed 30 June 2013).

Harmon, P. and Wolf, C. (2010), *The state of business process management* [Online], BPtrends. Available at http://www.bptrends.com/surveys_landing.cfm, (Accessed 30 June 2013).

Hartnett, D. (2007), *Text of letter on benefit records loss* [Online], British Broadcasting Corporation (BBC). Available at http://news.bbc.co.uk/1/hi/uk_politics/7107853.stm (Accessed 30 June 2013).

Herrmann, G. and Pernul, G. (1998), 'Towards security semantics in workflow management', *in Proceedings of the Thirty-First Hawaii International Conference on System Sciences (1998),* (7), pp. 766–767.

Herrmann, P. and Herrmann, G. (2006), 'Security requirement analysis of business processes', *Electron Commerce Research,* (6), pp. 305– 335.

HIPAA (1996), *Health Insurance Portability and Accountability Act of 1996*, Public Law 104-191, 104th Congress, USA.

Hogganvik, I. (2009), *A Graphical Approach to Security Risk Analysis*, PhD thesis, Faculty of Mathematics and Natural Sciences, University of Oslo.

Holz, H. J., Applin, A., Haberman, B., Joyce, D., Purchase, H. and Reed, C. (2006), 'Research methods in computing: what are they, and how should we teach them?', *in Working group reports on ITiCSE on Innovation and technology in computer science education (ITiCSE-WGR '06)*, ACM, New York, NY, USA, pp. 96–114. http://doi.acm.org/10.1145/1189215.1189180

IDS Scheer (1994), *ARIS* [Online], IDS Scheer. Available at http://www.aris.com (Accessed 30 June 2013).

Innerhofer–Oberperfler, F. and Breu, R. (2006), ‘Using an Enterprise Architecture for IT Risk Management’, *in Proceeding of Information Security South Africa Conference (ISSA’06), South Africa, 2006.*

Ioannidis, C., Pym, D. and Williams, J. (2012), ‘Investments and trade-offs in the economics of information security’, *European Journal of Operational Research*, 216 (2), pp. 424–444.

ISF (2005), *The Standard of Good Practice for Information Security V4.1*, Information Security Forum (ISF) [Online]. Available at https://www.securityforum.org/ (Accessed 30 June 2013).

Islam, M. M., Bhuiyan, M., Krishna, A. and Ghose, A. (2009), ‘An integrated approach to managing business process risk using rich organizational models’, *in Proceedings of the Confederated International Conferences, CoopIS, DOA, IS, and ODBASE 2009 on the Move to Meaningful Internet Systems: Part I’, OTM ’09,* Springer-Verlag, Berlin, Heidelberg, pp. 273–285. http://dx.doi.org/10.1007/978-3-642-05148-7_19

ISM3 (2007), *Information Security Management Maturity Model (ISM3)*, ISM3 Consortium [Online]. Available at http://www.ism3.com/ (Accessed 30 June 2013).

ISO (2002), *ISO Guide 73:2002 Risk Management*, International Organization of Standardization (ISO).

ISO (2004*a*), *ISO-IEC 15504 (SPICE)*, International Organization of Standardization (ISO).

ISO (2004*b*), *ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1:*

Concepts and models for information and communications technology security management, International Organization of Standardization (ISO).

ISO (2005*a*), *ISO 12207:2008 Systems and Software Engineering - Software life cycle processes*, International Organization of Standardization (ISO).

ISO (2005*b*), *ISO 17799:2000 Information technology - Security techniques - Code of practice for information security management*, International Organization of Standardization (ISO).

ISO (2005*c*), *ISO 17799:2005 Information technology - Security techniques - Code of practice for information security management*, International Organization of Standardization (ISO).

ISO (2005*d*), *ISO 27001:2005 Information technology - Security techniques - Information security management systems – Requirements*, International Organization of Standardization (ISO).

ISO (2005*e*), *ISO 27002 Information technology - Security techniques - Code of practice for information security management*, International Organization of Standardization (ISO).

ISO (2005f), *ISO 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*, International Organization of Standardization (ISO).

ISO (2009*a*), *ISO/IEC 31000:2009 Risk management — Principles and guidelines*, International Organization of Standardization (ISO).

ISO (2009*b*), *ISO/IEC 31010:2009 Risk management — Risk assessment techniques*, International Organization of Standardization (ISO).

ISO (2010), *ISO 27003:2010 Information technology - Security techniques - Information security management system implementation guidance*, International Organization of Standardization (ISO).

ISO (2011*a*), *ISO 27004:2009 Information technology - Security techniques - Information security management – Measurement*, International Organization of Standardization (ISO).

ISO (2011*b*), *ISO 27005:2008 Information technology - Security techniques - Information security risk management*, International Organization of Standardization (ISO).

ISO (2011*c*), *ISO 27005:2011 Information technology - Security techniques - Information security risk management*, International Organization of Standardization (ISO).

ISO (2011*d*), *ISO 27006:2011 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems*, International Organization of Standardization (ISO).

ISO (2011*e*), *ISO 27011:2008 Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*, International Organization of Standardization (ISO).

ISO (2011*f*), *ISO 27031:2011 Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity*, International Organization of Standardization (ISO).

ISO (2011*g*), *ISO 27033:2009 Information technology - Security techniques - Network security - Part 1: Overview and concepts*, International Organization of Standardization (ISO).

ISO (2011*h*), *ISO 27035:2011 Information technology - Security techniques - Information security incident management*, International Organization of Standardization (ISO).

ISO (2011*i*), *ISO 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002*, International Organization of Standardization (ISO).

ISO (2012), *ISO/IEC 27000:2012 Information technology — Security techniques — Information security management systems — Overview and vocabulary*, International Organization of Standardization (ISO).

ISSA (2004), *Generally Accepted Information Security Principles (GAISP)*, Information Systems Security Association (ISSA) [Online]. Available at https://www.issa.org/ (Accessed 30 June 2013).

ITGI (2007), *Control Objectives for Information and related Technology (COBIT)*, *Version 4.1*, IT Governance Institute (ITGI) [Online]. Available at http://www.isaca.org/COBIT/Pages/default.aspx (Accessed 23 June 2012).

Jackson, M. (2007), 'NII-OU Security Workshop',The Open University, November 2007.

Jackson, M. A. (1999), 'Problem analysis using small problem frames', *South African Computer Journal, Special Issue on WOFACS'98,* 22, pp. 47–60.

Jallow, A. K., Majeed, B., Kostas Vergidis, a. A. T. and Roy., R. (2007), 'Operational risk analysis in business processes', *BT Technology Journal,* 25, pp. 168–177. http://dx.doi.org/10.1007/s10550-007-0018-4

Janssen, H. (1998), *Integration der Bedrohungs- und Risikoanalyse in ein Vorgehensmodell fuer Geschaeftsprozess Modellierung und Workflow Management*, PhD thesis, Oldenbourg University.

Jorion, P. (2006), *Value at Risk: The New Benchmark for Managing Financial Risk (3rd ed.)*, McGraw-Hill Professional.

Jürjens, J. (2000), 'Secure information flow for concurrent processes'*, in Proceedings of Concur 2000, International Conference on Concurrency Theory,* Pennsylvania, 2000, LNCS 1877, Springer-Verlag.

Jürjens, J. (2002), 'UMLsec: extending UML for secure systems development', *in LNCS, ed*., 'UML 2002 - The Unified Modeling Language. Model Engineering, Languages, Concepts, and Tools. 5th International Conference', Vol. 2460, pp. 412–425.

Jürjens, J. (2005), *Secure Systems Development with UML*, Springer-Verlag, Heidelberg, 2005.

Jürjens, J. and Wimmel, G. (2001), 'Formally Testing Fail-Safety of Electronic Purse Protocols', *in Proceedings of 16th IEEE International Conference on Automated Software Engineering (ASE 2001),* IEEE Computer Society 2001, pp. 408-411.

Khanmohammadi, K. and Houmb, S. H. (2010), 'Business Process-Based Information Security Risk Assessment', *Fourth International Conference on Network and System Security,* pp. 199–206.

Kinney, W. R. (2003), *Research opportunities in internal auditing - chapter 5 auditing risk assessment and risk management process* [Online], The Institute of

Internal Auditors Research Foundation. Available at https://na.theiia.org (Accessed 5 May 2011).

Lambert, J. H., Jennings, R. K. and Joshi, N. N. (2006), 'Integration of Risk Identification with Business Process Models', *Systems Engineering* 9(3), pp. 187–198.

Landis, J. R. and Koch, G. G. (March 1977), 'The measurement of observer agreement for categorical data', *Biometrics* 33, No.1, pp. 159–174.

Lautieri, S., Cooper, D. and Jackson, D., eds (2005), 'SafSec: Commonalities Between Safety and Security Assurance', *in Proceedings of the Thirteenth Safety Critical Systems Symposium – Southampton*, February 2005 by Springer-Verlag London Ltd.

Liu, L., Yu, E. and Mylopoulos, J. (2002), 'Analyzing security requirements as relationships among strategic actors', *in Proceeding of 2nd Symposium on Requirements Engineering for Information SecuritySREIS 02,* Raleigh, North Carolina, Oktober 2002.

Luqi and Nogueira, J. (2000),' A risk assessment model for evolutionary software projects', *in Proceedings of the 2000 Monterey Workshop on Modelling Software System Structures in a fastly moving scenario*, Santa Margherita Ligure, 13-16 June 2000, Italy, pp. 208-216.

Luthy, D. and Forcht, K. (2006), 'Laws and regulations affecting information management and frameworks for assessing compliance', *Information Management & Computer Security* 14/2, pp. 155–166.

MAGERIT (2006), *Magerit – Version 2 Methodology for information systems risk analysis and management*, Spanish Ministry for Public Administrations [Online]. Available at http://administracionelectronica.gob.es (Accessed 30 June 2013).

Manadhata, P. and Wing, J. M. (2005), *An attack surface metric*, Carnegie Mellon University, CMU-CS-05-155.

Matulevicius, Mayer, Mouratidis, Dubois, Heymans and Genon (2008), 'Adapting secure tropos for security risk management in the early phases of information systems development', *CAISE 2008, Z. Bellahsene and M. Leonard (Eds.): CAiSE 2008, LNCS 5074* pp. 541–555.

Matulevicius, R., Mayer, N. and Heymans, P. (2008),' Alignment of misuse cases with security risk management', *in Proceedings of the 2008 Third International Conference on Availability, Reliability and Security ARES '08*, pp. 1397 – 1404.

Mayer, N. (2009), *Model-based Management of Information System Security Risk*, PhD thesis, Computer Science Department, University of Namur.

McDermott, J. and Fox, C. (1999), 'Using abuse case models for security requirements analysis'*, in Proceedings of the 15th Annual Computer Security Applications Conference*, IEEE Computer Society, Washington, DC, USA, p. 55.

McKenna, S. (2001), 'Organizational complexity and perceptions of risk', Risk Management 3/2, pp. 53–64.

Mead, N., Hough, E. and Stehney, T. (2005), *Security Quality Requirements Engineering (SQUARE) Methodology*, Software Engineering Institute (SEI), Carnegie Mellon University, CMU/SEI-2005-TR-009.

Mead and Stehney (2005), ‘Security quality requirements engineering (square) methodology’, *in Proceedings of the 2005 workshop on Software engineering for secure systems—building trustworthy applications (SESS05)*, New York, NY, USA.

Mendes, R., Mateus, J., Silva, E. and Tribolet, J. (2003), ‘Applying business process modeling to organizational change’, *in Proceedings of AMCIS 2003,* Paper 58, Tampa, Florida.

Mockel, C. and Abdallah, A. (2010), ‘Threat modeling approaches and tools for securing architectural designs of an e-banking application’, *in Proceedings of 2010 Sixth International Conference on Information Assurance and Security (IAS)*, pp. 149–154, Atlanta, GA.

Moffett, J. D., Haley, C. B. and Nuseibeh, B. (2004), *Core security requirements artefacts*, The Open University, TR 2004/23.

NASA (1966), *Procedure for Failure Mode, Effects, and Criticality Analysis (FMECA)*, National Aeronautics and Space Administration [Online]. Available at http://www.dtic.mil/dtic/tr/fulltext/u2/a278508.pdf (Accessed 30 June 2013).

Neiger, D., Churilov, L., zur Muehlen, M. and Rosemann, M. (2006),’ Integrating risks in business process models with value focused process engineering*’, in Proceedings of European Conference on Information Systems (ECIS) 2006,* Paper 122.

Neubauer, T., Klemen, M. and Biffl, S. (2005), ‘Business process-based valuation of IT-Security’, *in Proceedings of 7th International Workshop on Economics-Driven Software Engineering Research (EDSER’05)*, ACM, St. Louis, Missouri, USA.

OMG (2009), *Business Process Model and Notation (BPMN) FTF Beta 1 for Version 2.0*, Object Management Group (OMG) [Online]. Available at http://www.omg.org/ (Accessed 30 June 2013).

Paulk, M. C., Curtis, B., Chrissis, M. B. and Weber, C. V. (1993*), Capability maturity model for software Version 1.1*, Software Engineering Institute (SEI), Carnegie Mellon University, CMU/SEI-93-TR-024, ESC-TR-93-177.

Pfleeger, C. and Pfleeger, S. (2002), *Security in Computing*, Prentice Hall.

Phillips, C. and Swiler, L. P. (1998), 'A graph-based system for network-vulnerability analysis', *in Proceedings of the 1998 workshop on New security paradigms (NSPW 98),* Number 71-79, Charlottesville, VA, USA.

Pieters, W. and Consoli, L. (2009), 'Vulnerabilities and responsibilities: dealing with monsters in computer security', *Journal of Information, Communication & Ethics in Society,* Vol. 7 No. 4, pp. 243–257.

Pöttinger, J. (2009), *Self assessed risk management*, Master thesis, School of Informatics, Communications and Media, University of Applied Sciences Hagenberg, Upper Austria.

Putnam, A., Kreitner, C. and Rasmussen, M. (2004), *Information security management references* [Online], Corporate Information Security Working Group, United States House of Representatives, USA. Available at http://www.theiia.org/download.cfm?file=1319 (Accessed 30 June 2013).

Rainer, R.-K., Snyder, C. and Carr, H. (1991), 'Risk Analysis for Information Technology', *Journal of Management Information Systems,* 8(1), pp. 129–147.

Ralston, P., Graham, J. and Patel, S. (2006), *Literature review of security and risk assessment of SCADA and DCS systems*, Dept. of Computer Engineering and Computer Science, University of Louisville, TR-ISRL-06-01.

Rausand, M. (2004), *System Reliability Theory: Models, Statistical Methods, and Applications, 2nd Edition*, Wiley.

Redmill, F. (2002), 'Risk analysis - a subjective process', *Engineering Management Journal* 12(2), pp. 91–96.

Ribeiro, C. and Guedes, P. (1999), 'Verifying workflow processes against organization security policies', *in Proceedings of the 8th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, IEEE Computer Society*, pp. 190–191, Stanford, California.

Rikhardsson, P., Best, P., Green, P. and Rosemann, M. (2006*), Business process risk management, compliance and internal control: A research agenda, Working paper 2006-05* [Online], Department of Business Studies, Aarhus School of Business, University of Aarhus, Denmark. Available at http://www.hha.dk/bs/wp/man/M_2006_05.pdf (Accessed 30 June 2013).

Rinaldi, S., Peerenboom, J. and Kelly, T. (2001), 'Identifying, understanding, and analyzing critical infrastructure interdependencies', *Control Systems, IEEE* 21(6), pp. 11 –25.

Rodriguez, A., Fernandez-Medina, E. and Piattini, M. (2007), 'A BPMN extension for the modeling of security requirements in business processes', *IEICE - Transactions on Information and Systems*, E90-D(4), pp. 745–752.

Roehrig, S. (2003), *Using Process Models to Analyse IT Security Requirements*, PhD thesis, Zurich University.

Roehrig, S. and Knorr, K. (2004), 'Security analysis of electronic business processes', *Electronic Commerce Research,* 4, pp. 59–81.

Sarbanes-Oxley Act (2002), *Public Company Accounting Reform and Investor Protection Act of 2002* [Online], US Public Law 170-204. Available at http://beta.congress.gov/congressional-report/107th-congress/senate-report/205/1, (Accessed 30 June 2013).

Schneier, B. (1999), 'Attack trees', *Dr. Dobb's Journal,* 24(12), pp. 21–29.

Sindre, G. and Opdahl, A. L. (2005), 'Eliciting security requirements with misuse cases', *Requirements Engineering,* 10, pp. 34–44.

Siponen, M. T. (2005), 'An analysis of the traditional is security approaches: implications for research and practice', *European Journal of Information Systems,* 14, pp. 303–315.

Siponen, M. T. and Oinas-Kukkonen, H. (2007), 'A review of information security issues and respective research contributions', *The DATA BASE for Advances in Information Systems,* 38(1), pp. 60–80.

Siponen, M. and Willison, R. (2009), 'Information security management standards: Problems and solutions', *Information & Management,* 46, pp. 267–270.

Sjöberg, L., Moen, B.-E. and Rundmo, T. (2004), *Explaining risk perception, An evaluation of the psychometric paradigm in risk perception research* [Online], Norwegian University of Science and Technology, Department of Psychology, Trondheim, Norway, Rotunde publikasjoner. Available at http://paul-hadrien.info/backup/LSE/IS%20490/utile/Sjoberg%20Psychometric_paradigm.pdf (Accessed 30 June 2013).

Smith, G. W. (1990), ‘The semantic data model for security: Representing the security semantics of an application’, *in Proceedings of the 6th International Conference on Data Engineering*, pp. 322-329, Feb. 1990, Los Angeles, CA.

Sonnenreich, W., Albanese, J. and Stout, B. (2006), ‘Return on Security Investment (ROSI) – A Practical Quantitative Model’, *Journal of Research and Practice in Information Technology,* 38(1), pp. 55–66.

Stamatelatos, M. (2000*), Probabilistic risk assessment: What is it and why is it worth performing it?* [Online], National Aeronautics and Space Administration (NASA), Office of Safety and Mission Assurance. Available at http://www.hq.nasa.gov/office/codeq/qnews/pra.pdf (Accessed 30 June 2013).

Stelzer, D. (2002),‘ Risikoanalysen als Hilfsmittel zur Entwicklung von Sicherheitskonzepten in der Informationsverarbeitung‘, in *IT Sicherheitsmanagement in Banken*, Peter Roßbach, Hermann Locarek-Junge (Eds.), pp. 37–54.

Stevens, J. F. (2005), *Information asset profiling*, Software Engineering Institute (SEI), Carnegie Mellon University, CMU/SEI-2005-TN-021.

Stewart, A. (2004), ‘On risk: perception and direction’, *Computers & Security,* 23, pp. 362–370.

Stiglitz, J. E. (2008), *Making globalization work: Global financial markets in an era of turbulence* [Online], Institutional Money Congress, Frankfurt, February 19, 2008. Available at http://www2.gsb.columbia.edu/faculty/jstiglitz/speeches.cfm (Accessed 30 June 2013).

Stølen, K., den Braber, F., Dimitrakos, T., Fredriksen, R., Gran, B. A., Houmb, S.-H., Lund, M. S., Stamatiou, Y. C. and Øyvind Aagedal, J. (2002), ‘Model-based

risk assessment – the CORAS approach', *in Proceeding of Norsk Informatikk-konferanse 2002 (NIK'2002)*, Kongsberg, 25-27 Nov. 2002, Tapir forlag, pp. 239-249.

Stoneburner, G., Goguen, A. and Feringa, A. (2002*a*), *NIST Special Publication 800-123: Guide to general server security*, National Institute of Standards and Technology (NIST) [Online]. Available at http://www.nist.gov (Accessed 30 June 2013).

Stoneburner, G., Goguen, A. and Feringa, A. (2002*b*), *NIST Special Publication 800-30: Risk management guide for information technology systems*, National Institute of Standards and Technology (NIST) [Online]. Available at http://www.nist.gov (Accessed 30 June 2013).

Suh, B. and Han, I. (2003), 'The IS risk analysis based on a business model', *Information & Management,* 41, pp. 149 – 158.

Sun, L., Srivastava, R. and Mock, T. (2006), 'An information systems security risk assessment model under Dempster-Shafer theory of belief functions', *Journal of Management Information Systems,* 22(4), pp. 109 –142.

Sunyaev, A., Tremmel, F., Mauro, C., Leimeister, J. M. and Krcmar, H. (2009), 'A Reclassification of IS Security Analysis Approaches', *in Proceedings of the Fifteenth Americas Conference on Information Systems,* San Francisco, California August 6th-9th 2009.

Taubenberger, S., Juerjens, J., Yu, Y., Nuseibeh, B. (2013), 'Resolving Vulnerability Identification Errors using Security Requirements on Business Process Models', *Information Management & Computer Security*, Volume 21, Issue 3, pp.202 – 223.

Thoben, W. (1997), ‘Sicherheitsanforderungen im Rahmen der Bedrohungs und Risikoanalyse von IT-Systemen‘, in A. Geppert, Klaus R. Dittrich (Ed.) *Datenbanksysteme in Büro, Technik und Wissenschaft (BTW ’97*), Springer Publishing.

Tondel, I. A., Jaatun, M. G. and Meland, P. H. (2008), ‘Security requirements for the rest of us: A survey’, *IEEE Software,* 25(1), pp. 20–27.

Toval, A., Nicolás, J., Moros, B. and García, F. (2002), ‘Requirements reuse for improving information systems security: A practitioner’s approach’, *Requirements Engineering Journal,* 6, pp. 205–219.

UK DTI (1995), *BS7799:1995 - A code of practice for information security management*, Commercial Computer Security Centre (CCSC), UK Department of Trade and Industry's (DTI).

US DoD (1988), *Directive number 5200.28, Security Requirements for Automated Information Systems (AISs)* [Online], United States Department of Defense. Available at http://csrc.nist.gov/groups/SMA/fasp/documents/c&a/DLABSP/d520028p.pdf (Accessed 30 June 2013).

van Lamsweerde, A. and Letier, E. (2000), ‘Handling Obstacles in Goal-Oriented Requirements Engineering’, *in IEEE Transactions on Software Engineering, Special Issue on Exception Handling*, Vol. 26(10), pp. 978–1005.

Vidalis, S. (2004), *A critical discussion of risk and threat analysis methods and methodologies*, University of Glamorgan, Pontypridd, CS-04-03.

Viega, J. (2005), 'Building security requirements with CLASP', *in Proceedings of the 2005 workshop on Software engineering for secure systems (SESS '05) - building trustworthy applications*, New York, NY, USA, pp. 1–7.

Viera, A. J. and Garrett, J. M. (2005), 'Understanding interobserver agreement: The kappa statistic', *Family Medicine,* 37, No. 5, pp. 360–363.

von Solms, R. and von Solms, B. (2005), 'From information security to ... business security?', *Computers & Security*, (24), pp. 271–273.

Wallace, D. and Zelkowitz, M. V. (1997), 'Experimental validation in software engineering', *in Proceedings of Empirical Assessment & Evaluation in Software Engineering*, Special Issue: Evaluation & Assessment in Software Engineering, Information & Software Technology, 39(11), Keele University, Staffordshire, U.K.

Wang, A. J. A. (2005), 'Information security models and metrics', *in Proceedings of 43rd ACM Southeast Regional Conference 2005*, March 18-20, 2005, Kennesaw, GA, USA., Vol. 2 of *ACM-SE 43*, pp. 178–184.

Wang, C. and Wulf, W. A. (1997), 'Towards a framework for security measurement', *in Proceedings of 20th National Information Systems Security Conference (NISSC),* October 1997, Baltimore, MD.

Warren, M. J. (2001), 'A risk analysis model to reduce computer security risks among healthcare organizations', *Risk Management,* 3(1), pp. 27–37.

Wendler, R. (2012), 'The maturity of maturity model research: A systematic mapping study', *Information and Software Technology* Special Section on Software Reliability and Security, 54(12), pp. 1317 – 1339.

West, S. and Andrews, A. (2004), *OCTAVE-best practices comparative analysis, Advanced Technology Institute (ATI) as part of the Defense Healthcare*

Information Assurance Program (DHIAP), U.S. Army Medical Research and Materiel Command, TR 03-4.

Woodhouse, S. (2008),' An ISMS (Im)-Maturity Capability Model', *in Proceedings of the IEEE 8th International Conference on Computer and Information Technology Workshops*, CIT Workshops 2008, 8-11 July 2008, pp. 242 - 247, Sydney, QLD.

Yu, E. S. K. (1997), 'Towards modeling and reasoning support for early-phase requirements engineering', *in Proceedings of the 3rd IEEE International Symposium on Requirements Engineering (RE '97)*, IEEE Computer Society, Washington, DC, USA, pp. 226–235.

Yi-kun Zhang, Su-yang Jiang, Ying-an Cui, Yi-kun Zhang and Hui Xia (2010), 'A qualitative and quantitative risk assessment method in software security', *in Proceedings of 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, 2010, Vol. 1, pp. V1–534 –V1–539.

zur Muehlen, M. (2005), 'Integrating risks in business process models', *in Proceedings of the 16th Australasian Conference on Information Systems (ACIS 2005)*, Paper 50, Sydney.

zur Muehlen, M. (2007), *Class notes: BPM Research and Education* [Online], BPTrends. Available at http://www.bptrends.com (Accessed 30 June 2013).

zur Muehlen, M. and Ho, D. T.-Y. (2005), 'Risk Management in the BPM Lifecycle', *Business Process Management Workshops, Lecture Notes in Computer Science*, Vol. 3812, Springer Publishing, pp. 454–466.